SUSE Linux Enterprise Desktop

11 SP4

www.suse.com

14. Juli 2015

Administrationshandbuch



Administrationshandbuch

Inhaltsverzeichnis

Allgemeines zu diesem Handbuch xiii

1 Verfügbare Dokumentation xiv

2 Rückmeldungen xvi

3 Konventionen in der Dokumentation xvii

I Support und übliche Aufgaben 1

1 YaST-Online-Aktualisierung 3

1.1 Das Dialogfeld „Online-Aktualisierung“ 4

1.2 Installieren von Patches 8

1.3 Automatische Online-Updates 9

2 Erfassen der Systeminformationen für den Support 11

2.1 Erfassen von Systeminformationen mit supportconfig 11

2.2 Übertragen von Informationen an den globalen technischen Support 17

2.3 Unterstützung für Kernelmodule 19

2.4 Weiterführende Informationen 21

3 YaST im Textmodus 23

3.1 Navigation in Modulen 25

3.2 Einschränkung der Tastenkombinationen 27

3.3 YaST-Kommandozeilenoptionen 27

4 Snapshots/Rollback mit Snapper 31

4.1 Anforderungen 31

4.2 Rückgängigmachen von Systemänderungen mit Snapper 33

4.3 Manuelles Erstellen und Verwalten von Snapshots 45

4.4 Einschränkungen 50

4.5 Häufig gestellte Fragen 51

4.6 Verwenden von Snapper auf Thin Provisioned LVM-Volumes 52

5 Fernzugriff mit VNC 53

5.1 Einmalige VNC-Sitzungen 53

5.2 Permanente VNC-Sitzungen 56

6 GNOME-Konfiguration für Administratoren 61

6.1 Das GConf-System 61

6.2 Anpassen von Hauptmenü, Kontrollleiste und Application Browser 64

6.3 Automatischer Start von Anwendungen 65

6.4 Automatisches Einhängen und Verwalten von Mediengeräten 65

6.5 Ändern von bevorzugten Anwendungen 65

6.6 Verwalten von Profilen mit Sabayon 66

6.7 Hinzufügen von Dokumentvorlagen 71

6.8 Desktop-Sperrfunktionen 71

6.9 Weiterführende Informationen 72

7 Verwalten von Software mit Kommandozeilen-Tools 73

7.1 Verwenden von zypper 73

7.2 RPM - der Paket-Manager 90

8 Bash-Shell und Bash-Skripte 103

8.1 Was ist „die Shell“? 103

8.2 Schreiben von Shell-Skripten 110

8.3 Umlenken von Kommandoereignissen 111
8.4 Verwenden von Aliassen 113
8.5 Verwenden von Variablen in der Bash-Shell 113
8.6 Gruppieren und Kombinieren von Kommandos 116
8.7 Arbeiten mit häufigen Ablaufkonstrukten 117
8.8 Weiterführende Informationen 118

9 Using Third-Party Software 121

II System 123

10 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung 125

10.1 Laufzeitunterstützung 126
10.2 Software-Entwicklung 127
10.3 Software-Kompilierung auf Doppelarchitektur-Plattformen 127
10.4 Kernel-Spezifikationen 128

11 Booten und Konfigurieren eines Linux-Systems 131

11.1 Der Linux-Bootvorgang 131
11.2 Der `init`-Vorgang 135
11.3 Systemkonfiguration über `/etc/sysconfig` 145

12 Der Bootloader GRUB 151

12.1 Booten mit GRUB 152
12.2 Konfigurieren des Bootloaders mit YaST 164
12.3 Deinstallieren des Linux-Bootloaders 170
12.4 Erstellen von Boot-CDs 171
12.5 Der grafische SUSE-Bildschirm 172
12.6 Fehlersuche 173

12.7 Weiterführende Informationen 174

13 UEFI (Unified Extensible Firmware Interface) 177

13.1 Secure Boot 178

13.2 Weiterführende Informationen 186

14 Spezielle Systemfunktionen 189

14.1 Informationen zu speziellen Softwarepaketen 189

14.2 Virtuelle Konsolen 197

14.3 Tastaturzuordnung 197

14.4 Sprach- und länderspezifische Einstellungen 198

15 Druckerbetrieb 205

15.1 Work-Flow des Drucksystems 207

15.2 Methoden und Protokolle zum Anschließen von Druckern 207

15.3 Installation der Software 208

15.4 Netzwerkdrucker 209

15.5 Drucken über die Kommandozeile 212

15.6 Besondere Funktionen in SUSE Linux Enterprise Desktop 212

15.7 Fehlersuche 215

16 Gerätemanagement über dynamischen Kernel mithilfe von `udev` 225

16.1 Das `/dev`-Verzeichnis 225

16.2 Kernel-`uevents` und `udev` 226

16.3 Treiber, Kernel-Module und Geräte 227

16.4 Booten und erstes Einrichten des Geräts 227

16.5 Überwachen des aktiven `udev`-Daemons 228

16.6 Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von `udev`-Regeln 230

16.7 Permanente Gerätebenennung 238
16.8 Von `udev` verwendete Dateien 239
16.9 Weiterführende Informationen 239

17 Das X Window-System 241

17.1 Manuelles Konfigurieren des X Window-Systems 241
17.2 Installation und Konfiguration von Schriften 250
17.3 Weiterführende Informationen 256

18 Zugriff auf Dateisysteme mit FUSE 257

18.1 Konfigurieren von FUSE 257
18.2 Erhältliche FUSE-Plug-Ins 257
18.3 Weiterführende Informationen 258

III Mobile Computer 259

19 Mobile Computernutzung mit Linux 261

19.1 Notebooks 261
19.2 Mobile Hardware 270
19.3 Mobiltelefone und PDAs 271
19.4 Weiterführende Informationen 271

20 Wireless LAN 273

20.1 WLAN-Standards 273
20.2 Betriebsmodi 274
20.3 Authentifizierung 275
20.4 Verschlüsselung 277
20.5 Konfiguration mit YaST 278
20.6 Tipps und Tricks zur Einrichtung eines WLAN 287
20.7 Fehlersuche 289

20.8 Weiterführende Informationen 291

21 Energieverwaltung **293**

21.1 Energiesparfunktionen 293

21.2 Advanced Configuration & Power Interface (ACPI) 294

21.3 Ruhezustand für Festplatte 297

21.4 Fehlersuche 299

21.5 Weiterführende Informationen 301

22 Verwenden von Tablet PCs **303**

22.1 Installieren der Tablet PC-Pakete 304

22.2 Konfigurieren des Tablet-Geräts 305

22.3 Verwenden der virtuellen Tastatur 305

22.4 Drehen der Ansicht 306

22.5 Verwenden der Bewegungserkennung 307

22.6 Aufzeichnen von Notizen und Skizzen mit dem Pen 309

22.7 Fehlersuche 311

22.8 Weiterführende Informationen 313

IV Services **315**

23 Grundlegendes zu Netzwerken **317**

23.1 IP-Adressen und Routing 321

23.2 IPv6 – Das Internet der nächsten Generation 324

23.3 Namensauflösung 335

23.4 Konfigurieren von Netzwerkverbindungen mit YaST 337

23.5 NetworkManager 360

23.6 Manuelle Netzwerkkonfiguration 362

23.7 Einrichten von Bonding-Geräten 380

23.8 smpppd als Einwählhelfer 384

24 SLP-Dienste im Netzwerk 387

24.1 Installation 387
24.2 SLP aktivieren 388
24.3 SLP-Frontends in SUSE Linux Enterprise Desktop 388
24.4 Bereitstellen von Diensten über SLP 389
24.5 Weiterführende Informationen 390

25 Zeitsynchronisierung mit NTP 391

25.1 Konfigurieren eines NTP-Client mit YaST 392
25.2 Manuelle Konfiguration von NTP im Netzwerk 396
25.3 Dynamische Zeitsynchronisierung während der Laufzeit 397
25.4 Einrichten einer lokalen Referenzuhr 398

26 Verwendung von NetworkManager 399

26.1 Anwendungsbeispiele für den NetworkManager 399
26.2 Aktivieren oder Deaktivieren von NetworkManager 400
26.3 Konfigurieren von Netzwerkverbindungen 401
26.4 Verwenden von KNetworkManager 404
26.5 Verwenden des GNOME NetworkManager-Miniprogramme 410
26.6 NetworkManager und VPN 413
26.7 NetworkManager und Sicherheit 414
26.8 Häufig gestellte Fragen 416
26.9 Fehlersuche 418
26.10 Weiterführende Informationen 419

27 Samba 421

27.1 Terminologie 421
27.2 Konfigurieren eines Samba-Servers 423

27.3 Konfigurieren der Clients 423
27.4 Samba als Anmeldeserver 424
27.5 Weiterführende Informationen 425

28 Verteilte Nutzung von Dateisystemen mit NFS 427

28.1 Terminologie 427
28.2 Installieren des NFS-Servers 428
28.3 Konfigurieren des NFS-Servers 428
28.4 Konfigurieren der Clients 429
28.5 Weiterführende Informationen 433

29 Dateisynchronisierung 435

29.1 Verfügbare Software zur Datensynchronisierung 435
29.2 Kriterien für die Auswahl eines Programms 437
29.3 Einführung in CVS 440
29.4 Einführung in rsync 443
29.5 Weiterführende Informationen 445

V Fehlersuche 447

30 Hilfe und Dokumentation 449

30.1 Dokumentationsverzeichnis 450
30.2 man-Seiten 452
30.3 Infoseiten 453
30.4 Online-Ressourcen 454

31 Häufige Probleme und deren Lösung 457

31.1 Suchen und Sammeln von Informationen 457
31.2 Probleme bei der Installation 461
31.3 Probleme beim Booten 472

31.4 Probleme bei der Anmeldung 476

31.5 Probleme mit dem Netzwerk 485

31.6 Probleme mit Daten 490

A Ein Beispielnetzwerk 509

B GNU Licenses 511

B.1 GNU Free Documentation License 511



Allgemeines zu diesem Handbuch

Dieses Handbuch ist für professionelle Netzwerk- und Systemadministratoren zum Betrieb von SUSE® Linux Enterprise konzipiert. Daher soll es nur sicherstellen, dass SUSE Linux Enterprise korrekt konfiguriert ist und die erforderlichen Dienste im Netzwerk verfügbar sind, um eine ordnungsgemäße Funktion gemäß der ursprünglichen Installation zu erlauben. Dieses Handbuch behandelt nicht, wie Sie dafür sorgen, dass SUSE Linux Enterprise die geeignete Kompatibilität mit der Anwendungssoftware Ihres Unternehmens bietet oder dass seine Kernfunktionalität diese Anforderungen erfüllt. Das Handbuch setzt voraus, dass eine vollständige Anforderungsüberprüfung durchgeführt und die Installation angefordert wurde bzw. dass eine Testinstallation zum Zwecke einer solchen Überprüfung angefordert wurde.

Diese Handbuch enthält Folgendes:

Support und übliche Aufgaben
: SUSE Linux Enterprise bietet eine breite Palette an Werkzeugen, um verschiedene Aspekte des Systems anzupassen. In diesem Abschnitt werden einige dieser Aspekte erläutert.

System
: In diesem Abschnitt wird das zugrunde liegende Betriebssystem umfassend erläutert. SUSE Linux Enterprise unterstützt eine Reihe von Hardware-Architekturen, mit denen Sie Ihre eigenen Anwendungen anpassen können, die auf SUSE Linux Enterprise ausgeführt werden sollen. Der Bootloader und die Informationen zum Bootvorgang unterstützen Sie dabei zu verstehen, wie Ihr Linux-System arbeitet und wie sich Ihre eigenen Skripten und Anwendungen integrieren lassen.

Mobile Computer
: Laptops und die Kommunikation zwischen mobilen Geräten wie PDAs oder Mobiltelefonen und SUSE Linux Enterprise benötigen eine gewisse Aufmerksamkeit. Achten Sie auf geringen Energieverbrauch und sorgen Sie für die Integration verschiedener Geräte in einer sich ändernden Netzwerkumgebung. Machen Sie sich auch mit den Hintergrundtechnologien vertraut, die die erforderliche Funktionalität liefern.

Services
: SUSE Linux Enterprise ist als Netzwerk-Betriebssystem konzipiert. SUSE® Linux Enterprise Desktop bietet Client-Unterstützung für viele Netzwerkdienste. Es lässt sich gut in heterogene Umgebungen mit MS Windows-Clients und -Servern integrieren.

Fehlersuche
: Bietet einen Überblick zu Hilfeinformationen und zusätzlicher Dokumentation, falls Sie weitere Informationen benötigen oder mit Ihrem System spezifische Aufgaben ausführen möchten. In diesem Teil werden die häufigsten Probleme und Störungen zusammengestellt und Sie erfahren, wie Sie diese Probleme selbst beheben können.

Viele Kapitel in diesem Handbuch enthalten Links zu zusätzlichen Dokumentationsressourcen. Dazu gehört auch weitere Dokumentation, die auf dem System bzw. im Internet verfügbar ist.

Einen Überblick über die Dokumentation, die für Ihr Produkt verfügbar ist, und die neuesten Dokumentationsupdates finden Sie unter `http://www.suse.com/doc`.

1 Verfügbare Dokumentation

Wir stellen Ihnen unsere Handbücher in verschiedenen Sprachen in den Formaten HTML und PDF zur Verfügung. Die folgenden Handbücher für Benutzer und Administratoren sind für dieses Produkt verfügbar:

KDE User Guide (↑*KDE User Guide*)
: Einführung in den KDE-Desktop von SUSE Linux Enterprise Desktop. Das Handbuch begleitet Sie bei der Verwendung und Konfiguration des Desktops und hilft Ihnen, wichtige Aufgaben zu erledigen. Es richtet sich in erster Linie an Endbenutzer, die KDE als ihren Standard-Desktop nutzen.

GNOME-Benutzerhandbuch (↑*GNOME-Benutzerhandbuch*)
: Einführung in den GNOME-Desktop von SUSE Linux Enterprise Desktop. Das Handbuch begleitet Sie bei der Verwendung und Konfiguration des Desktops und hilft Ihnen, wichtige Aufgaben zu erledigen. Es richtet sich in erster Linie an Endbenutzer, die den GNOME-Desktop als ihren Standard-Desktop nutzen möchten.

Anwendungshandbuch (↑*Anwendungshandbuch*)
: Erfahren Sie, wie wichtige Desktop-Anwendungen unter SUSE Linux Enterprise Desktop konfiguriert werden. Dieses Handbuch bietet eine Einführung in Browser und E-Mail-Clients sowie Büro-Anwendungen und Tools für die Zusammenarbeit. Es behandelt auch Grafik- und Multimedia-Anwendungen.

Bereitstellungshandbuch (↑*Bereitstellungshandbuch*)
: Erfahren Sie, wie Sie einzelne oder mehrere Systeme installieren und die Produktfunktionen für eine Bereitstellungsinfrastruktur nutzen. Wählen Sie aus verschiedenen Ansätzen. Von der lokalen Installation über einen Netzwerkinstallationsserver bis zu einer Masseninstallation über eine entfernt gesteuerte, hochgradig angepasste und automatisierte Installationsmethode ist alles möglich.

Administrationshandbuch (S. i)
: Er behandelt Systemverwaltungsaufgaben wie Wartung, Überwachung und Anpassung eines neu installierten Systems.

Security Guide (↑*Security Guide*)
: Zudem werden grundlegende Konzepte der Systemsicherheit vorgestellt, die sowohl lokale als auch netzwerkbezogene Aspekte abdecken. Sie erfahren, wie Sie die einem Produkt inhärente Sicherheitssoftware wie AppArmor verwenden können (diese ermöglicht es Ihnen, für jedes Programm einzeln festzulegen, für welche Dateien Lese-, Schreib- und Ausführungsberechtigungen bestehen) und das Prüfsystem nutzen können, das zuverlässig Daten zu sicherheitsrelevanten Ereignissen sammelt.

System Analysis and Tuning Guide (↑*System Analysis and Tuning Guide*)
: Ein Administratorhandbuch zur Problemsuche, Fehlerbehebung und Optimierung. Erfahren Sie, wie Sie Ihr System mithilfe von Überwachungswerkzeugen prüfen und optimieren können und wie Sie Ihre Ressourcen effizient verwalten. Es enthält zudem einen Überblick über häufige Probleme und Lösungen sowie weitere Hilfequellen und Dokumentationsressourcen.

Virtualization with Xen (↑*Virtualization with Xen*)
: Enthält eine Einführung in die Virtualisierungstechnologie Ihres Produkts. Es bietet einen Überblick über die zahlreichen Anwendungsmöglichkeiten und Installationstypen für jede von SUSE Linux Enterprise Server unterstützte Plattform sowie eine Kurzbeschreibung des Installationsvorgangs.

Neben den umfangreichen Handbüchern stehen Ihnen auch verschiedene Schnelleinführungen zur Verfügung:

KDE Quick Start (↑*KDE Quick Start*)
: Bietet eine kurze Einführung in den KDE-Desktop und einige wichtige Anwendungen, die darauf ausgeführt werden.

GNOME Quick Start (↑*GNOME Quick Start*)
: Bietet eine kurze Einführung in den GNOME-Desktop und einige wichtige Anwendungen, die darauf ausgeführt werden.

LibreOffice.org Quick Start (↑*LibreOffice.org Quick Start*)
: Bietet eine kurze Einführung in die LibreOffice-Suite und deren Module zum Schreiben von Text, zum Arbeiten mit Tabellenkalkulationen oder zum Erstellen von Grafiken und Präsentationen.

Schnelleinführung zur Installation (↑*Schnelleinführung zur Installation*)
: Listet die Systemanforderungen auf und führt Sie schrittweise durch die Installation von SUSE Linux Enterprise Desktop von DVD oder einem ISO-Abbild.

Linux Audit Quick Start
: Vermittelt einen kurzen Überblick über die Aktivierung und Konfiguration des Prüfsystems und die Ausführung der wichtigsten Aufgaben wie die Einrichtung von Prüfregeln, die Generierung von Berichten und die Analyse der Protokolldateien.

AppArmor Quick Start
: Dient dem Verständnis der wichtigsten Konzepte von AppArmor®.

HTML-Versionen der meisten Produkthandbücher finden Sie auf dem installierten System im Verzeichnis `/usr/share/doc/manual` bzw. in den Hilfezentren Ihres Desktops. Die neuesten Dokumentationsaktualisierungen finden Sie unter http://www.suse.com/doc, von wo Sie PDF- oder HTML-Versionen der Handbücher für Ihr Produkt herunterladen können.

2 Rückmeldungen

Für Rückmeldungen stehen mehrere Kanäle zur Verfügung:

Fehler und Verbesserungsanforderungen
: Informationen zu Diensten und Support-Optionen, die für Ihr Produkt verfügbar sind, finden Sie unter `http://www.suse.com/support/`.

  Um Fehler für eine Produktkomponente zu melden, melden Sie sich über `http://www.suse.com/support/` beim Novell Customer Center an und wählen Sie die Optionsfolge *My Support (Mein Support)* > *Service Request (Service-Anforderung)*.

Anregungen und Kritik unserer Leser
: Wir freuen uns über Ihre Kommentare und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation dieses Produkts. Verwenden Sie die Funktion „Benutzerkommentare" unten auf den einzelnen Seiten der Online-Dokumentation oder geben Sie Ihre Kommentare auf der Seite `http://www.suse.com/doc/feedback.html` ein.

Mail
: Für Feedback zur Dokumentation dieses Produkts können Sie auch eine E-Mail an `doc-team@suse.de` senden. Geben Sie auf jeden Fall auch den Titel der Dokumentation, die Produktversion und das Datum der Veröffentlichung der Dokumentation an. Geben Sie eine genaue Beschreibung des Problems an und beziehen Sie sich auf die entsprechende Abschnittsnummer und Seite (oder URL), wenn Sie Fehler melden oder Verbesserungen vorschlagen.

3 Konventionen in der Dokumentation

In diesem Handbuch werden folgende typografische Konventionen verwendet:

- `/etc/passwd`: Verzeichnisnamen und Dateinamen
- *`Platzhalter`*: Ersetzen Sie *`Platzhalter`* durch den tatsächlichen Wert.
- `PATH`: die Umgebungsvariable PATH
- `ls`, `--help`: Kommandos, Optionen und Parameter

- `Benutzer`: Benutzer oder Gruppen
- Alt, Alt + F1: Eine Taste oder Tastenkombination. Tastennamen werden wie auf der Tastatur in Großbuchstaben dargestellt.
- *Datei*, *Datei* > *Speichern unter*: Menüelemente, Schaltflächen
- *Tanzende Pinguine* (Kapitel *Pinguine*, ↑Zusätzliches Handbuch): Dies ist ein Verweis auf ein Kapitel in einem anderen Handbuch.

Teil I. Support und übliche Aufgaben



1 YaST-Online-Aktualisierung

Novell stellt fortlaufend Sicherheitsupdates für Ihr Softwareprodukt bereit. Standardmäßig stellt das Miniprogramm für die Aktualisierung sicher, dass Ihr System stets auf dem neuesten Stand ist. Weitere Informationen zu diesem Miniprogramm finden Sie im Abschnitt „Halten Sie Ihr System auf dem neuesten Stand“ (Kapitel 6, *Installieren bzw. Entfernen von Software*, ↑*Bereitstellungshandbuch*). Dieses Kapitel behandelt das alternative Tool für die Aktualisierung von Software-Paketen: die YaST-Online-Aktualisierung.

Die aktuellen Patches für SUSE® Linux Enterprise Desktop sind über ein Software-Aktualisierungs-Repository verfügbar. Wenn Sie Ihr Produkt während der Installation registriert haben, ist das Aktualisierungs-Repository bereits konfiguriert. Wenn Sie SUSE Linux Enterprise Desktop nicht registriert haben, können Sie *Software* > *Online-Update-Konfiguration* in YaST ausführen und *Erweitert* > *Für Support registrieren und Aktualisierungs-Repository beziehen* starten. Alternativ können Sie ein Aktualisierungs-Repository manuell von einer verbürgten Quelle hinzufügen. Starten Sie zum Hinzufügen oder Entfernen von Repositorys den Repository-Manager über *Software* > *Software-Repositorys* in YaST. Weitere Informationen zum Repository Manager finden Sie in Abschnitt „Verwalten von Software-Repositorys und -Diensten“ (Kapitel 6, *Installieren bzw. Entfernen von Software*, ↑*Bereitstellungshandbuch*).

ANMERKUNG: Fehler beim Zugriff auf den Aktualisierungskatalog

Wenn Sie keinen Zugriff auf den Aktualisierungskatalog erhalten, liegt das eventuell daran, dass Ihr Abo abgelaufen ist. In der Regel umfasst SUSE Linux Enterprise Desktop ein einjähriges oder dreijähriges Abo, mit dem Sie Zugriff

auf den Aktualisierungskatalog erhalten. Dieser Zugriff wird verweigert, sobald das Abo beendet ist.

Bei Verweigerung des Zugriffs auf den Aktualisierungskatalog wird eine Warnmeldung angezeigt, die Ihnen empfiehlt, das Novell Customer Center zu besuchen und Ihr Abo zu überprüfen. Das Novell Customer Center finden Sie unter `http://www.novell.com/center/`.

---

bietet Aktualisierungen mit verschiedenen Relevanzstufen:

Sicherheits-Updates
: Beseitigen ernsthafte Sicherheitsrisiken und sollten auf jeden Fall installiert werden.

Empfohlene Updates
: Beseitigen Probleme, die Ihrem Rechner schaden können.

Optionale Updates
: Beseitigen nicht sicherheitsrelevante Probleme oder bieten Verbesserungen.

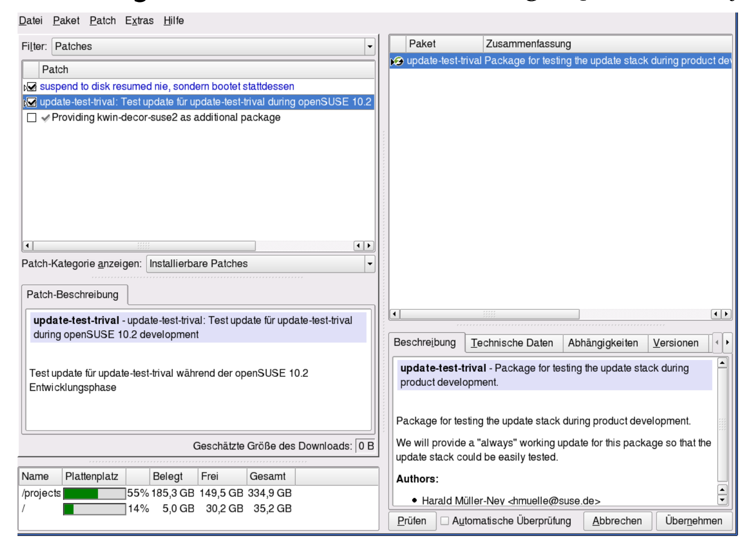
1.1 Das Dialogfeld „Online-Aktualisierung“

Das YaST-Dialogfeld *Online-Aktualisierung* ist in zwei Toolkit-Varianten verfügbar: GTK (für GNOME) und Qt (für KDE). Beide Bedienoberflächen unterscheiden sich zwar im Erscheinungsbild, bieten jedoch im Prinzip dieselben Funktionen. Die folgenden Abschnitte enthalten eine kurze Beschreibung der einzelnen Funktionen. Zum Öffnen des Dialogfelds starten Sie YaST und wählen Sie *Software* > *Online-Aktualisierung*. Stattdessen können Sie es auch von der Kommandozeile aus mit dem Kommando `yast2 online_update` starten.

1.1.1 KDE-Bedienoberfläche (Qt)

Das Fenster *Online-Update* ist in vier Abschnitte unterteilt.

Abbildung 1.1 *YaST-Online-Aktualisierung – Qt-Bedienoberfläche*



Unter *Zusammenfassung* im linken Bereich werden die verfügbaren Patches für SUSE Linux Enterprise Desktop aufgeführt. Die Patches werden nach Sicherheitsrelevanz (`Sicherheit`, `Empfohlen` und `Optional`) sortiert. Sie können die Ansicht des Abschnitts *Zusammenfassung* ändern, indem Sie eine der folgenden Optionen unter *Patch-Kategorie anzeigen* auswählen:

Erforderliche Patches (Standardansicht)
: Nicht installierte Patches für Pakete, die auf Ihrem System installiert sind.

Nicht erforderliche Patches
: Patches für Pakete, die nicht auf Ihrem System installiert sind, oder Patches, die nicht mehr erforderlich sind (weil die relevanten Pakete bereits von einer anderen Quelle aktualisiert wurden).

Alle Patches
: Alle verfügbaren Patches für SUSE Linux Enterprise Desktop.

Jeder Listeneintrag im Abschnitt *Zusammenfassung* besteht aus einem Symbol und dem Patch-Namen. Eine Übersicht der möglichen Symbole und deren Bedeutung erhalten Sie, wenn Sie die Taste Umschalttaste + F1 drücken. Die erforderlichen Aktionen für Patches der Kategorie `Sicherheit` und `Empfohlen` sind automatisch voreingestellt.

Möglich sind die Aktionen *Automatisch installieren*, *Automatisch aktualisieren* und *Automatisch löschen*.

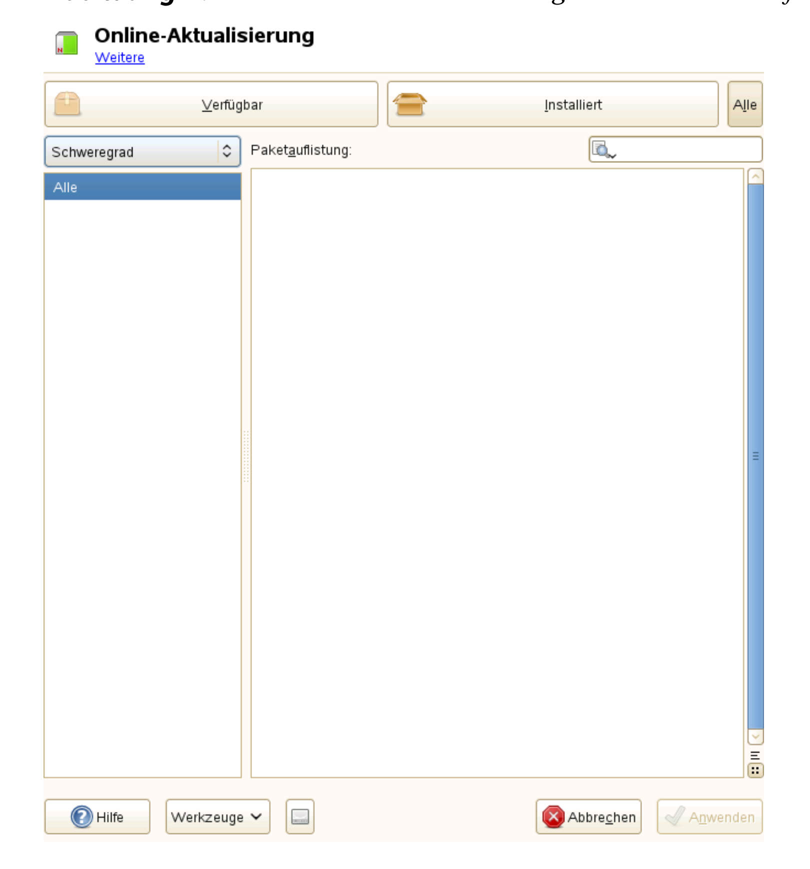
Wenn Sie ein aktuelles Paket aus einem anderen als dem Aktualisierungs-Repository installieren, können die Anforderungen eines Patches für dieses Paket mit dieser Installation erfüllt sein. In diesem Fall wird ein Häkchen vor der Patchzusammenfassung angezeigt. Das Patch wird in der Liste angezeigt, bis Sie es für die Installation kennzeichnen. Dadurch wird nicht das Patch installiert (da das Paket bereits aktuell ist), sondern das Patch als installiert gekennzeichnet.

Wählen Sie einen Eintrag im Abschnitt *Zusammenfassung* aus, um eine kurze *Patch-Beschreibung* unten links im Dialogfeld anzuzeigen. Im Abschnitt oben rechts werden die Pakete aufgeführt, die im ausgewählten Patch enthalten sind (ein Patch kann aus mehreren Paketen bestehen). Klicken Sie im Abschnitt oben rechts auf einen Eintrag, um Details zu dem entsprechenden Paket, das im Patch enthalten ist, anzuzeigen.

1.1.2 GNOME-Bedienoberfläche (GTK)

Das Fenster *Online-Aktualisierung* ist in vier Hauptabschnitte unterteilt.

Abbildung 1.2 *YaST-Online-Aktualisierung – GTK-Bedienoberfläche*



Im Abschnitt oben rechts werden die verfügbaren (oder bereits installierten) Patches für SUSE Linux Enterprise Desktop aufgeführt. Zum Filtern der Patches nach Sicherheitsrelevanz klicken Sie auf den entsprechenden Eintrag *Priorität* oben rechts im Fenster: `Sicherheit`, `Empfohlen`, `Optional` oder `Alle Patches`.

Wenn alle verfügbaren Patches bereits installiert sind, werden unter *Package listing* (Paketliste) im Abschnitt rechts oben keine Einträge angezeigt. Das Feld im Abschnitt unten links zeigt die Anzahl der verfügbaren und der bereits installierten Patches an und ermöglicht ein Umschalten der Ansicht auf *Verfügbar* oder *Installiert*.

Wählen Sie einen Eintrag im Abschnitt *Paketliste* aus, um eine Patch-Beschreibung und weitere Details unten rechts im Dialogfeld anzuzeigen. Da ein Patch aus mehreren

Paketen bestehen kann, klicken Sie auf den Eintrag *Gültig für* im Abschnitt unten rechts, um festzustellen, welche Pakete im entsprechenden Patch enthalten sind.

Klicken Sie auf einen Patch-Eintrag, um eine Zeile mit detaillierten Informationen zu dem Patch im unteren Fensterbereich anzuzeigen. Hier sehen Sie eine detaillierte Beschreibung für den Patch sowie die verfügbaren Versionen. Sie können auf *Installieren* klicken, um optionale Patches zu installieren; Sicherheitspatches und empfohlene Patches sind bereits zur Installation vorausgewählt.

1.2 Installieren von Patches

Im YaST-Dialogfeld „Online-Aktualisierung“ können Sie entweder alle verfügbaren Patches in einem Schritt installieren oder die Patches, die Sie auf Ihr System anwenden möchten, manuell auswählen. Außerdem können Sie Patches, die auf das System angewendet wurden, zurücksetzen.

Standardmäßig sind alle neuen Patches (außer den `optionalen`), die derzeit für Ihr System verfügbar sind, bereits zur Installation markiert. Sie werden automatisch angewendet, sobald Sie auf *Übernehmen* oder *Anwenden* klicken.

Prozedur 1.1 *Anwenden von Patches mit der YaST-Online-Aktualisierung*

1 Starten Sie YaST, und wählen Sie *Software* > *Online-Aktualisierung*.

2 Um alle neuen Patches automatisch anzuwenden (mit Ausnahme der `optionalen` Patches), die zurzeit für Ihr System verfügbar sind, klicken Sie auf *Anwenden* oder *Übernehmen*, um die Installation der vorab ausgewählten Patches zu starten.

3 So ändern Sie zunächst die Auswahl der Patches, die Sie anwenden möchten:

3a Verwenden Sie die entsprechenden Filter und Ansichten, die die GTK- und Qt-Bedienoberflächen bereitstellen. Detaillierte Informationen finden Sie unter Abschnitt 1.1.1, „KDE-Bedienoberfläche (Qt)“ (S. 4) und Abschnitt 1.1.2, „GNOME-Bedienoberfläche (GTK)“ (S. 6).

3b Wählen Sie Patches Ihren Anforderungen und Wünschen entsprechend aus oder heben Sie die Auswahl auf, indem Sie das entsprechende Kontrollkästchen aktivieren oder deaktivieren (GNOME) oder indem Sie mit der rechten

Maustaste auf den Patch klicken und die gewünschte Aktion im Kontextmenü auswählen (KDE).

WICHTIG: Anwenden von Sicherheits-Updates ohne Ausnahme

Heben Sie die Auswahl der `sicherheitsrelevanten` Patches nicht ohne stichhaltigen Grund auf. Diese Patches beseitigen ernsthafte Sicherheitsrisiken und schützen Ihr System vor Angriffen.

3c Die meisten Patches umfassen Aktualisierungen für mehrere Pakete. Wenn Sie Aktionen für einzelne Pakete ändern möchten, klicken Sie mit der rechten Maustaste auf eine Paketansicht und wählen Sie eine Aktion (KDE).

3d Bestätigen Sie Ihre Auswahl, und wenden Sie die ausgewählten Patches mit *Anwenden* oder *Übernehmen* an.

4 Klicken Sie nach abgeschlossener Installation auf *Beenden*, um das YaST-Dialogfeld *Online-Aktualisierung* zu verlassen. Ihr System ist nun auf dem neuesten Stand.

TIPP: Deaktivieren von deltarpms

Standardmäßig werden Aktualisierungen als deltarpms heruntergeladen. Da der Neuaufbau von rpm-Paketen aus deltarpms eine speicher- und prozessorintensive Aufgabe ist, können bestimmte Setups oder Hardwarekonfigurationen das Deaktivieren der deltarpms-Verwendung aus Leistungsgründen erfordern.

Zum Deaktivieren der Verwendung von deltarpms bearbeiten Sie die Datei `/etc/zypp/zypp.conf` und legen Sie `download.use_deltarpm` auf `false` fest.

1.3 Automatische Online-Updates

YaST bietet außerdem die Möglichkeit, eine automatische Aktualisierung mit täglichem, wöchentlichem oder monatlichem Zeitplan einzurichten. Um das entsprechende Modul zu verwenden, müssen Sie zunächst das Paket `yast2-online-update-configuration` installieren.

Prozedur 1.2 *Konfigurieren des automatischen Online-Updates*

1 Nach der Installation starten Sie YaST, und wählen Sie *Software* > *Einrichtung der Online-Aktualisierung*.

Sie können das Modul auch mit dem Kommando `yast2 online_update_configuration` von der Kommandozeile aus starten.

2 Aktivieren Sie die Option *Automatische Online-Aktualisierung*.

3 Wählen Sie aus, ob das Update *Täglich*, *Wöchentlich* oder *Monatlich* ausgeführt werden soll.

Einige Patches, z. B. Kernel-Updates oder Pakete mit Lizenzvereinbarungen, erfordern Benutzerinteraktion, wodurch der automatische Aktualisierungsprozess angehalten würde.

4 Wählen Sie aus, ob Sie *Interaktive Patches überspringen* möchten, für den Fall, dass der Aktualisierungsprozess vollständig automatisch fortgesetzt werden soll.

WICHTIG: Überspringen von Patches

Wenn Sie Pakete, die Benutzerinteraktion erfordern, überspringen, führen Sie regelmäßig eine manuelle *Online-Aktualisierung* aus, um diese Patches ebenfalls zu installieren. Andernfalls entgehen Ihnen möglicherweise wichtige Patches.

---

5 Damit Lizenzvereinbarungen automatisch akzeptiert werden, aktivieren Sie die Option *Lizenzen zustimmen*.

6 Sollen alle Pakete automatisch installiert werden, die durch die aktualisierten Pakete empfohlen werden, aktivieren Sie *Empfohlene Pakete einbeziehen*.

7 Sollen die Patches nach Kategorie gefiltert werden (z. B. Sicherheits-Patches oder empfohlene Patches), aktivieren Sie *Nach Kategorie filtern*, und fügen Sie die entsprechenden Patch-Kategorien aus der Liste ein. Es werden nur Patches aus den ausgewählten Kategorien installiert. Andere werden übersprungen.

8 Bestätigen Sie die Konfiguration mit *OK*.

Erfassen der Systeminformationen für den Support

2

Bei Problemen wird ein detaillierter Systembericht mit dem Kommandozeilenwerkzeug `supportconfig` oder mit dem YaST-*Support*-Modul erzeugt. Beide Werkzeuge sammeln Informationen zum System, beispielsweise aktuelle Kernel-Version, Hardware, installierte Pakete, Partitionseinrichtung und einiges mehr. Hierbei wird ein TAR-Archiv mit Dateien ausgegeben. Wenn Sie eine Service-Anforderung öffnen, können Sie das TAR-Archiv für den globalen technischen Support heraufladen. Der Support hilft Ihnen, das gemeldete Problem zu lokalisieren und zu beheben.

Das Kommandozeilenwerkzeug wird im Paket `supportutils` bereitgestellt, das standardmäßig installiert ist. Das YaST-*Support*-Modul baut auf dem Kommandozeilenwerkzeug auf.

2.1 Erfassen von Systeminformationen mit supportconfig

Zum Erstellen eines TAR-Archivs mit detaillierten Systeminformationen, die Sie an den globalen technischen Support übertragen können, verwenden Sie entweder direkt das Kommandozeilenwerkzeug `supportconfig` oder das YaST-*Support*-Modul. Das Kommandozeilenwerkzeug wird im Paket `supportutils` bereitgestellt, das standardmäßig installiert ist. Das YaST-*Support*-Modul baut zudem auf dem Kommandozeilenwerkzeug auf.

2.1.1 Erstellen einer Serviceanforderungsnummer

supportconfig-Archive können jederzeit erzeugt werden. Wenn Sie die supportconfig-Daten an den globalen technischen Support übertragen möchten, müssen Sie jedoch zunächst eine Service-Anforderungs-Nummer erstellen. Diese Nummer benötigen Sie, um das Archiv an den Support heraufladen zu können.

Zum Erstellen einer Service-Anforderung wechseln Sie zu `http://www.novell.com/center/eservice`, und befolgen Sie die Anweisungen auf dem Bildschirm. Schreiben Sie sich die 11-stellige Service-Anforderungs-Nummer auf.

ANMERKUNG: Datenschutzerklärung

SUSE und Novell behandeln die Systemberichte als vertraulich. Weitere Informationen zum Datenschutz finden Sie unter `http://www.novell.com/company/legal/privacy/`.

2.1.2 Upload-Ziele

Sobald Sie eine Service-Anforderungs-Nummer erstellt haben, können Sie Ihre supportconfig-Archive gemäß den Anweisungen in Prozedur 2.1, „Übertragen von Informationen an den Support mithilfe von YaST“ (S. 17) oder Prozedur 2.2, „Übertragen von Informationen an den Support über die Kommandozeile“ (S. 18) an den globalen technischen Support heraufladen. Verwenden Sie eines der folgenden Upload-Ziele:

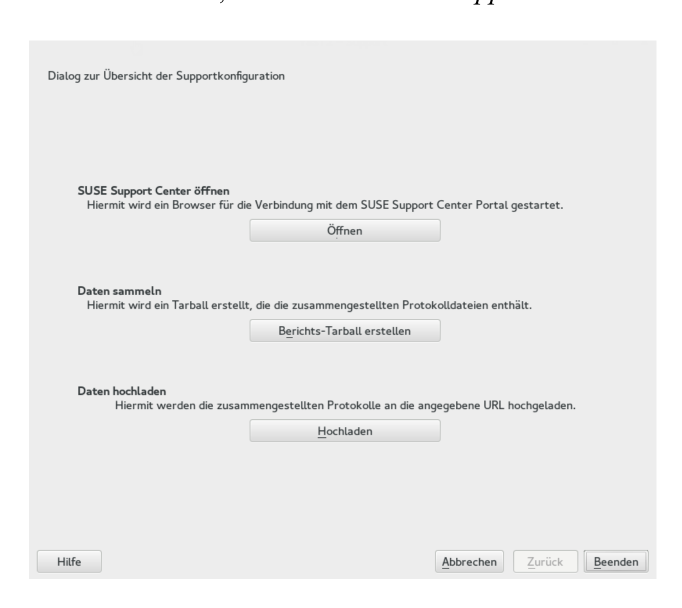
- Kunden in den USA: `ftp://ftp.novell.com/incoming`
- EMEA (Europa, Nahost und Afrika): `ftp://support-ftp.suse.com/in`

Alternativ können Sie das TAR-Archiv auch an Ihre Service-Anforderung anhängen und die URL für Service-Anforderungen verwenden: `http://www.novell.com/center/eservice`.

2.1.3 Erstellen eines supportconfig-Archivs mit YaST

Gehen Sie wie folgt vor, wenn Sie Ihre Systeminformationen mithilfe von YaST erfassen möchten:

1 Starten Sie YaST, und öffnen Sie das *Support*-Modul.



2 Klicken Sie auf *Berichts-Tarball erstellen*.

3 Wählen Sie im nächsten Fenster eine der supportconfig-Optionen in der Optionsliste aus. Die Option *Benutzerdefinierte Einstellungen (für Experten) verwenden* ist standardmäßig aktiviert. Wenn Sie die Berichtfunktion zuerst testen möchten, verwenden Sie *Nur eine minimale Anzahl von Informationen sammeln*. Weitere Hintergrundoptionen zu den weiteren Optionen finden Sie auf der man-Seite zu `supportconfig`.

Fahren Sie mit *Weiter* fort.

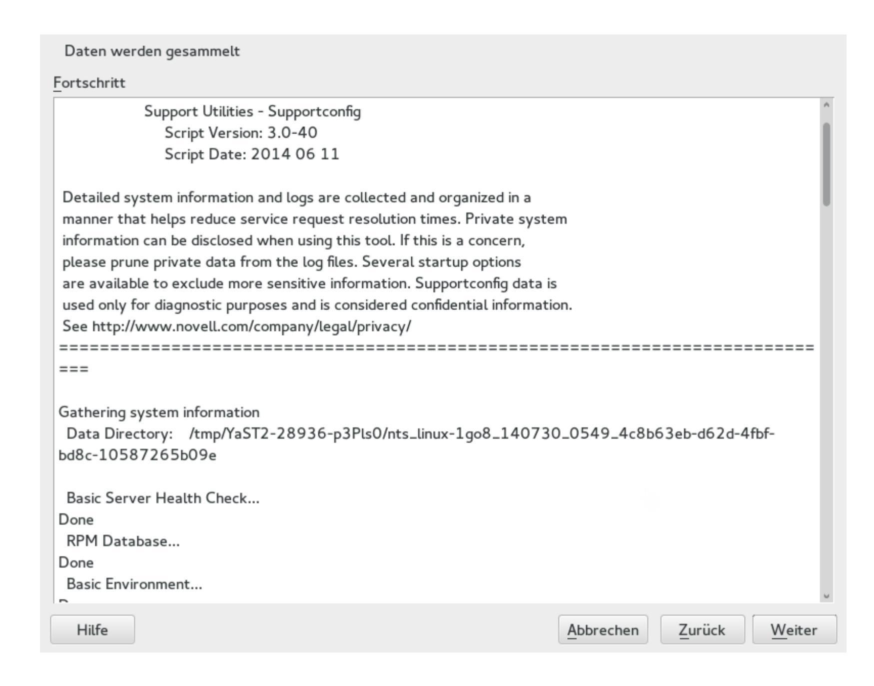
4 Geben Sie Ihre Kontaktdaten ein. Die Daten werden in die Datei `basic-environment.txt` geschrieben und in das zu erstellende Archiv aufgenommen.

5 Soll das Archiv nach Abschluss der Datenerfassung an den globalen technischen Support gesendet werden, müssen Sie *Upload-Informationen* angeben. YaST schlägt automatisch einen Upload-Server vor. Wenn Sie diesen Server ändern möchten, erfahren Sie in Abschnitt 2.1.2, „Upload-Ziele“ (S. 12), welche Upload-Server verfügbar sind.

Soll das Archiv erst später gesendet werden, können Sie die *Upload-Informationen* leer lassen.

6 Fahren Sie mit *Weiter* fort.

7 Es wird nun mit dem Sammeln der Informationen begonnen.



Fahren Sie nach Ende des Vorgangs mit *Weiter* fort.

8 Prüfen der Datensammlung: Wählen Sie den *Dateinamen* einer Protokolldatei aus. Der Inhalt dieser Datei wird in YaST angezeigt. Entfernen Sie bei Bedarf die

Dateien, die nicht in das TAR-Archiv aufgenommen werden sollen, mit *Aus Daten entfernen*. Fahren Sie mit *Weiter* fort.

9. Speichern Sie das TAR-Archiv. Wenn Sie das YaST-Modul als `root`-Benutzer gestartet hatten, schlägt YaST standardmäßig den Ordner `/var/log` als Speicherort für das Archiv vor (ansonsten Ihr Benutzerverzeichnis). Das Format des Dateinamens lautet `nts_`*`HOST_DATUM_UHRZEIT`*`.tbz`.

10. Soll das Archiv direkt an den Support heraufgeladen werden, muss die Aktion *Protokolldatei-Tarball an URL heraufladen* aktiviert sein. Hier ist das *Upload-Ziel* angegeben, das YaST in Schritt 5 (S. 14) vorgeschlagen hat. Wenn Sie das Upload-Ziel ändern möchten, erfahren Sie in Abschnitt 2.1.2, „Upload-Ziele“ (S. 12), welche Upload-Server verfügbar sind.

11. Um das Heraufladen zu überspringen, deaktivieren Sie die Option *Protokolldatei-Tarball zu URL heraufladen*.

12. Bestätigen Sie die Änderungen. Das YaST-Modul wird geschlossen.

2.1.4 Erstellen eines supportconfig-Archivs über die Kommandozeile

Mit dem nachstehenden Verfahren erstellen Sie ein supportconfig-Archiv, ohne das Archiv direkt an den Support zu übertragen. Zum Heraufladen müssen Sie das entsprechende Kommando mit den zugehörigen Optionen ausführen (siehe Prozedur 2.2, „Übertragen von Informationen an den Support über die Kommandozeile“ (S. 18)).

1. Öffnen Sie eine Shell und melden Sie sich als `root` an.

2. Führen Sie `supportconfig` ohne Optionen aus. Damit werden die Standard-Systeminformationen gesammelt.

3. Warten Sie, bis das Tool den Vorgang beendet hat.

4. Der Standardspeicherort für das Archiv befindet sich unter `/var/log` und hat das Dateinamenformat `nts_`*`HOST_DATUM_UHRZEIT`*`.tbz`.

2.1.5 Allgemeine Optionen für Supportconfig

Das Dienstprogramm `supportconfig` wird in der Regel ohne Optionen aufgerufen. Zeigen Sie mit eine Liste aller Optionen für `supportconfig` mit `-h` an oder lesen Sie die man-Seite. Die folgende Liste enthält eine kurze Übersicht einiger gängiger Fälle:

Vermindern des Umfangs der erfassten Informationen
: Verwenden Sie die Minimal-Option (`-m`):

```
supportconfig -m
```

Begrenzen der Informationen auf ein bestimmtes Thema
: Wenn Sie in der standardmäßigen `supportconfig`-Ausgabe bereits ein Problem festgestellt haben und dieses Problem auf einen bestimmten Bereich oder eine bestimmte Funktionsgruppe beschränkt ist, können Sie die erfassten Informationen beim nächsten Ausführen von `supportconfig` auf diesen Bereich begrenzen. Wenn Sie beispielsweise ein Problem mit LVM erkannt haben und daher eine Änderung testen möchten, die Sie vor Kurzem an der LVM-Konfiguration hatten, reicht es völlig aus, nur die minimalen supportconfig-Informationen zu LVM zu erfassen:

```
supportconfig -i LVM
```

Eine vollständige Liste der Funktionsschlüsselwörter, mit denen Sie die erfassten Informationen auf einen bestimmten Bereich begrenzen, erhalten Sie mit dem

```
supportconfig -F
```

Aufnehmen zusätzlicher Kontaktinformationen in die Ausgabe:

```
supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

(alle in einer Zeile)

Sammeln von bereits rotierten Protokolldateien

```
supportconfig -l
```

Dies ist insbesondere in Umgebungen mit hohem Protokollierungsaufkommen nützlich, und außerdem nach einem Kernel-Crash, wenn syslog die Protokolldateien nach dem Neubooten rotiert.

2.2 Übertragen von Informationen an den globalen technischen Support

Zum Übertragen der Systeminformationen an den globalen technischen Support verwenden Sie das YaST-*Support*-Modul oder das Befehlszeilenprogramm `supportconfig`. Falls Serverprobleme auftreten und Sie Hilfe benötigen, müssen Sie zunächst eine Serviceanforderung öffnen. Weitere Informationen finden Sie unter Abschnitt 2.1.1, „Erstellen einer Serviceanforderungsnummer" (S. 12).

In den nachfolgenden Beispielen fungiert die Zahl *`12345678901`* als Platzhalter für die Service-Anforderungs-Nummer. Ersetzen Sie die Zahl *`12345678901`* durch die Service-Anforderungs-Nummer, die Sie in Abschnitt 2.1.1, „Erstellen einer Serviceanforderungsnummer" (S. 12) erstellt haben.

Prozedur 2.1 *Übertragen von Informationen an den Support mithilfe von YaST*

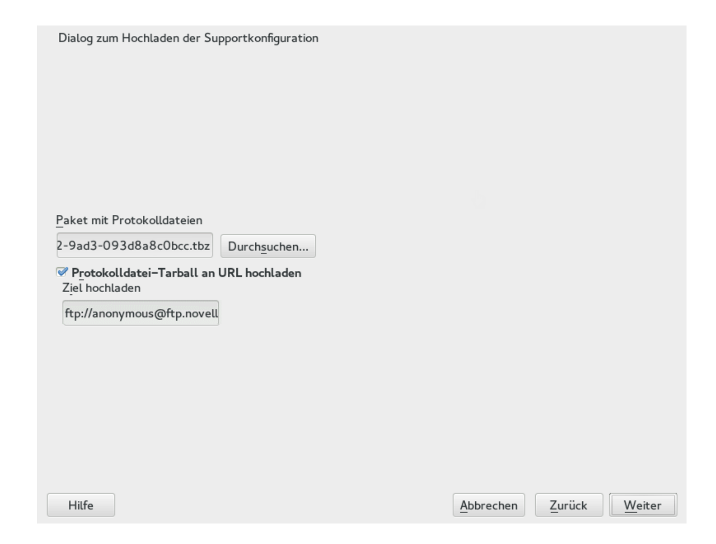
Im nachfolgenden Verfahren wird angenommen, dass Sie bereits ein supportconfig-Archiv erstellt, jedoch noch nicht heraufgeladen haben. Nehmen Sie in jedem Fall Ihre Kontaktdaten in das Archiv auf (siehe Abschnitt 2.1.3, „Erstellen eines supportconfig-Archivs mit YaST" (S. 13), Schritt 4). Weitere Anweisungen zum Erzeugen und Übertragen eines supportconfig-Archivs in einem einzigen Arbeitsgang finden Sie in Abschnitt 2.1.3, „Erstellen eines supportconfig-Archivs mit YaST" (S. 13).

1 Starten Sie YaST, und öffnen Sie das *Support*-Modul.

2 Klicken Sie auf *Heraufladen*.

3 Geben Sie unter *Paket mit Protokolldateien* den Pfad zum vorhandenen supportconfig-Archiv ein, oder klicken Sie auf *Durchsuchen*, und wechseln Sie zu dem Ordner, in dem sich das Archiv befindet.

4 YaST schlägt automatisch einen Upload-Server vor. Wenn Sie diesen Server ändern möchten, erfahren Sie in Abschnitt 2.1.2, „Upload-Ziele" (S. 12), welche Upload-Server verfügbar sind.



Fahren Sie mit *Weiter* fort.

5 Klicken Sie auf *Fertig stellen*.

Prozedur 2.2 *Übertragen von Informationen an den Support über die Kommandozeile*

Im nachfolgenden Verfahren wird angenommen, dass Sie bereits ein supportconfig-Archiv erstellt, jedoch noch nicht heraufgeladen haben. Weitere Anweisungen zum Erzeugen und Übertragen eines supportconfig-Archivs in einem einzigen Arbeitsgang finden Sie in Abschnitt 2.1.3, „Erstellen eines supportconfig-Archivs mit YaST“ (S. 13).

1 Server mit Internetkonnektivität:

1a Führen Sie das folgende Kommando aus, um das Standard-Uploadziel zu verwenden:

```
supportconfig -ur 12345678901
```

1b Verwenden Sie das folgende sichere Upload-Ziel:

```
supportconfig -ar 12345678901
```

2 Server *ohne* Internetkonnektivität

2a Führen Sie Folgendes aus:

```
supportconfig -r 12345678901
```

2b Laden Sie das Archiv `/var/log/nts_SR12345678901*tbz` manuell auf einen unserer FTP-Server herauf. Der richtige Server ist abhängig von Ihrem Standort. Einen Überblick finden Sie unter Abschnitt 2.1.2, „Upload-Ziele“ (S. 12).

3 Sobald sich das TAR-Archiv im Eingangsverzeichnis unseres FTP-Servers befindet, wird es automatisch an Ihre Service-Anforderung angehängt.

2.3 Unterstützung für Kernelmodule

Eine wichtige Anforderung für jedes Enterprise-Betriebssystem ist der Grad der Unterstützung für die jeweilige Umgebung. Kernelmodule sind die wichtigsten Bindeglieder zwischen der Hardware („Controller“) und dem Betriebssystem. Die Kernelmodule in SUSE Linux Enterprise umfassen jeweils das Flag `supported`, das drei mögliche Werte annehmen kann:

- „Ja“, daher `supported`
- „Extern“, daher `supported`
- „“ (leer, nicht festgelegt), daher `unsupported`

Es gelten die folgenden Regeln:

- Alle Module eines selbst rückkompilierten Kernels sind standardmäßig als nicht unterstützt gekennzeichnet.
- Kernelmodule, die von den SUSE-Partnern unterstützt und über das `SUSE SolidDriver-Programm` bereitgestellt, sind als „extern“ gekennzeichnet.
- Wenn das Flag `supported` nicht gesetzt ist, wird der Kernel beim Laden dieses Moduls unbrauchbar. Unbrauchbare Kernel werden nicht unterstützt. Nicht unterstützte Kernelmodule befinden sich in einem separaten RPM-Paket (`kernel-FLAVOR-extra`) und werden nicht standardmäßig geladen

(*FLAVOR*=default||xen|...). Darüber hinaus sind diese nicht unterstützten Module im Installationsprogramm nicht verfügbar, und das Kernelpaket `kernel-FLAVOR-extra`ist kein Bestandteil der SUSE Linux Enterprise-Medien.

- Kernelmodule, die nicht unter einer zur Lizenz des Linux-Kernels kompatiblen Lizenz bereitgestellt werden, machen den Kernel ebenfalls unbrauchbar. Weitere Informationen finden Sie unter `/usr/src/linux/Documentation/sysctl/kernel.txt` und dem Status `/proc/sys/kernel/tainted`.

2.3.1 Technischer Hintergrund

- Linux-Kernel: Der Standardwert für `/proc/sys/kernel/unsupported` bei SUSE Linux Enterprise 11 SP4 lautet `2` (`do not warn in syslog when loading unsupported modules`; keine Warnung im Syslog, wenn nicht unterstützte Module geladen werden). Dieser Standardwert wird sowohl im Installationsprogramm als auch im installierten System verwendet. Weitere Informationen finden Sie unter `/usr/src/linux/Documentation/sysctl/kernel.txt`.

- `modprobe`: Das Dienstprogramm `modprobe` zum Prüfen der Modulabhängigkeiten und zum Laden der Module prüft den Wert des Flags `supported`. Beim Wert „Ja" oder „Extern" wird das Modul geladen, ansonsten nicht. Weitere Informationen, wie Sie dieses Verhalten außer Kraft setzen, finden Sie in Abschnitt 2.3.2, „Arbeiten mit nicht unterstützten Modulen" (S. 20).

ANMERKUNG

SUSE bietet im Allgemeinen keine Unterstützung für das Entfernen von Speichermodulen mit `modprobe -r`.

2.3.2 Arbeiten mit nicht unterstützten Modulen

Die allgemeine Unterstützung ist wichtig. Dennoch können Situationen eintreten, in denen ein nicht unterstütztes Modul erforderlich ist (beispielsweise zu Testzwecken, für die Fehlersuche oder wenn der Hardware-Hersteller ein HotFix bereitstellt).

- Zum Überschreiben des Standardwerts bearbeiten Sie die Datei /etc/modprobe.d/unsupported-modules.conf und ändern Sie den Wert der Variablen allow_unsupported_modules in 1. Falls in der initrd ein nicht unterstütztes Modul erforderlich ist, müssen Sie zur Aktualisierung der initrd auch mkinitrd ausführen.

  Falls Sie nur einmalig versuchen möchten, ein Modul zu laden, verwenden Sie die Option --allow-unsupported-modules für modprobe. Weitere Informationen finden Sie auf der man-Seite zu modprobe.

- Während der Installation werden nicht unterstützte Module u. U. über Treiberaktualisierungs-Datenträger hinzugefügt und entsprechend geladen. Soll das Laden von nicht unterstützten Modulen beim Booten und zu späteren Zeitpunkten erzwungen werden, verwenden Sie die Kernel-Kommandozeile oem-modules. Beim Installieren und Initialisieren des Pakets module-init-tools wird das Kernel-Flag TAINT_NO_SUPPORT (/proc/sys/kernel/tainted) ausgewertet. Ist das Kernel bereits unbrauchbar, wird allow_unsupported_modules aktiviert. Damit wird verhindert, dass nicht unterstützte Module im zu installierenden System zu Fehlern führen. Wenn während der Installation keine nicht unterstützten Module vorhanden sind und die andere spezielle Kernel-Kommandozeilenoption (oem-modules=1) nicht verwendet wird, so werden die nicht unterstützten Module dennoch standardmäßig nicht zugelassen.

Beachten Sie, dass der Kernel und das gesamte System nicht mehr durch SUSE unterstützt werden, sobald nicht unterstützte Module geladen und ausgeführt werden.

2.4 Weiterführende Informationen

Weitere Informationen zum Erfassen von Systeminformationen finden Sie in den folgenden Dokumenten:

- man supportconfig – man-Seite zu supportconfig.

- man supportconfig.conf – man-Seite zur supportconfig-Konfigurationsdatei.

- http://www.suse.com/communities/conversations/basic-server-health-check-supportconfig/ – Grundlegende Server-Integritätsprüfung mit supportconfig.

- https://www.novell.com/communities/coolsolutions/cool_tools/create-your-own-supportconfig-plugin/ – Erstellen eines eigenen supportconfig-Plug-ins.

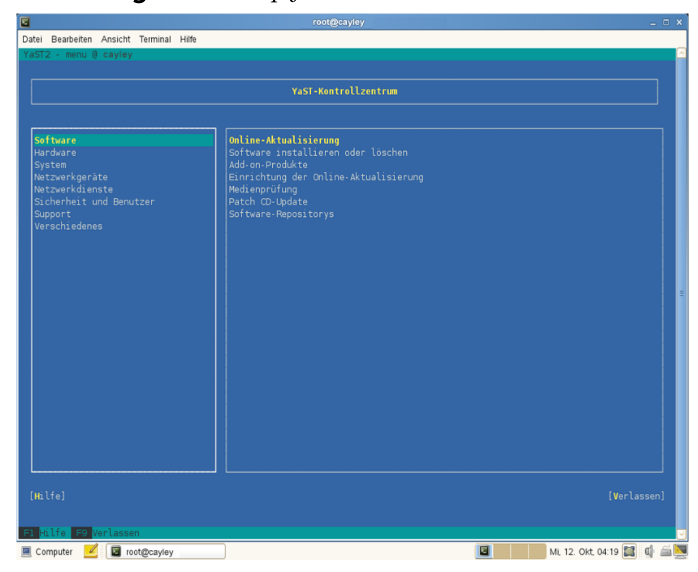
- http://www.suse.com/communities/conversations/creating-a-central-supportconfig-repository/ – Erstellen eines zentralen supportconfig-Repositorys.

3 YaST im Textmodus

Dieser Abschnitt richtet sich an Systemadministratoren und Experten, die keinen X-Server auf Ihren Systemen ausführen und daher auf das textbasierte Installationswerkzeug angewiesen sind. Der Abschnitt enthält grundlegende Informationen zum Start und Betrieb von YaST im Textmodus.

YaST verwendet im Textmodus die ncurses-Bibliothek, um eine bequeme pseudografische Bedienoberfläche zu bieten. Die ncurses-Bibliothek wird standardmäßig installiert. Die minimale unterstützte Größe des Terminal-Emulators, in dem Sie YaST ausführen, beträgt 80 x 25 Zeichen.

Abbildung 3.1 *Hauptfenster von YaST im Textmodus*



Wenn Sie YaST im Textmodus starten, wird das YaST-Kontrollzentrum angezeigt (siehe Abbildung 3.1). Das Hauptfenster besteht aus drei Bereichen. Der linke Bereich zeigt die Kategorien, denen die verschiedenen Module angehören. Dieser Bereich ist beim Start von YaST aktiv und wird daher durch eine breite weiße Umrandung gekennzeichnet. Die aktive Kategorie ist markiert. Der linke Bereich bietet einen Überblick über die Module, die in der aktiven Kategorie zur Verfügung stehen. Der untere Bereich enthält die Schaltflächen für *Hilfe* und *Verlassen*.

Wenn Sie das YaST-Kontrollzentrum starten, wird automatisch die Kategorie *Software* ausgewählt. Mit ↓ und ↑ können Sie die Kategorie ändern. Zum Auswählen eines Moduls aus der Kategorie aktivieren Sie den rechten Bereich mit und wählen Sie dann das Modul mit ↓ und ↑ aus. Halten Sie die Pfeiltasten gedrückt, um durch die Liste der verfügbaren Module zu blättern. Der ausgewählte Eintrag wird markiert. Drücken Sie Eingabetaste, um das aktive Modul zu starten.

Zahlreiche Schaltflächen oder Auswahlfelder im Modul enthalten einen markierten Buchstaben (standardmäßig gelb) Mit Alt + markierter_Buchstabe können Sie eine Schaltfläche direkt auswählen und müssen nicht mit Tabulator zu der Schaltfläche wechseln. Zum Verlassen des YaST-Kontrollzentrums drücken Sie Alt + Q; alternativ wählen Sie *Verlassen* und drücken Sie Eingabetaste.

TIPP: Aktualisieren des YaST-Dialogfelds

Wenn ein YaST-Dialogfeld verzerrt oder unleserlich wird (z. B. beim Ändern der Fenstergröße), drücken Sie Strg + L. Damit wird das Fenster aktualisiert und der Fensterinhalt wird wiederhergestellt.

3.1 Navigation in Modulen

Bei der folgenden Beschreibung der Steuerelemente in den YaST-Modulen wird davon ausgegangen, dass alle Kombinationen aus Funktionstasten und Alt-Taste funktionieren und nicht anderen globalen Funktionen zugewiesen sind. In Abschnitt 3.2, „Einschränkung der Tastenkombinationen“ (S. 27) finden Sie Informationen zu möglichen Ausnahmen.

Navigation zwischen Schaltflächen und Auswahllisten
: Verwenden Sie Tab, um zwischen den Schaltflächen und Einzelbildern mit den Auswahllisten zu navigieren. Zum Navigieren in umgekehrter Reihenfolge verwenden Sie die Tastenkombinationen Alt + Tab oder Umschalttaste + Tab.

Navigation in Auswahllisten
: Mit den Pfeiltasten (↑ und ↓) können Sie zwischen den einzelnen Elementen in einem aktiven Rahmen, der eine Auswahlliste enthält, navigieren. Wenn einzelne Einträge innerhalb eines Rahmens dessen Breite überschreiten, können Sie mit Umschalttaste + → oder Umschalttaste + ← horizontal nach rechts bzw. links blättern. Alternativ können Sie Strg + E oder Strg + A verwenden. Diese Kombination kann auch verwendet werden, wenn → oder ← zu einem Wechsel des aktiven Rahmens oder der aktuellen Auswahlliste führt, wie dies im Kontrollzentrum der Fall ist.

Schaltflächen, Optionsschaltfläche und Kontrollkästchen
: Um Schaltflächen mit leeren eckigen Klammern (Kontrollkästchen) oder leeren runden Klammern (Optionsschaltflächen) auszuwählen, drücken Sie die Leertaste oder Eingabetaste. Alternativ können Optionsschaltflächen und Kontrollkästchen unmittelbar mit Alt + markierter_Buchstabe ausgewählt werden. In diesem Fall brauchen Sie die Auswahl nicht mit Eingabetaste zu bestätigen . Wenn Sie mit Tabulator zu einem Element wechseln, können Sie durch Drücken von Eingabetaste die ausgewählte Aktion ausführen bzw. das betreffende Menüelement aktivieren.

Funktionstasten
: Die F-Tasten (F1 bis F12) bieten schnellen Zugriff auf die verschiedenen Schaltflächen. Verfügbare F-Tastenkürzel werden in der untersten Zeile des YaST-Bildschirms angezeigt. Welche Funktionstasten welchen Schaltflächen zugeordnet sind, hängt vom aktiven YaST-Modul ab, da die verschiedenen Module unterschiedliche Schaltflächen aufweisen (Details, Info, Hinzufügen, Löschen usw.). F10 wird für *Übernehmen*, *OK*, *Weiter* und *Beenden* verwendet. Drücken Sie F1, um Zugriff auf die YaST-Hilfe zu erhalten.

Verwenden der Navigationsstruktur im ncurses-Modus
: Einige YaST-Module bieten im linken Fensterbereich eine Navigationsstruktur, in der Konfigurationsdialogfenster ausgewählt werden können. Mit den Pfeiltasten (und) können Sie in der Baumstruktur navigieren. Drücken Sie die Leertaste, um Elemente der Struktur zu öffnen oder zu schließen. Im ncurses-Modus muss nach einer Auswahl in der Navigationsstruktur die Taste Eingabetaste gedrückt werden, um das ausgewählte Dialogfeld anzuzeigen. Dieses beabsichtigte Verhalten erspart zeitraubende Bildaufbauvorgänge beim Blättern durch die Navigationsstruktur.

Abbildung 3.2 *Das Software-Installationsmodul*

3.2 Einschränkung der Tastenkombinationen

Wenn der Fenster-Manager globale Alt-Kombinationen verwendet, funktionieren die Alt-Kombinationen in YaST möglicherweise nicht. Tasten wie Alt oder Umschalttaste können auch durch die Einstellungen des Terminals belegt sein.

Ersetzen von Alt durch Esc
: Tastenkombinationen mit Alt können auch mit Esc anstelle von Alt ausgeführt werden. Esc – H beispielsweise ersetzt Alt + H. (Drücken Sie zunächst Esc, und drücken Sie *dann* H.)

Navigation vor und zurück mit Strg + F und Strg + B
: Wenn die Kombinationen mit Alt und Umschalttaste vom Fenster-Manager oder dem Terminal belegt sind, verwenden Sie stattdessen die Kombinationen Strg + F (vor) und Strg + B (zurück).

Einschränkung der Funktionstasten
: Die F-Tasten werden auch für Funktionen verwendet. Bestimmte Funktionstasten können vom Terminal belegt sein und stehen eventuell für YaST nicht zur Verfügung. Auf einer reinen Textkonsole sollten die Tastenkombinationen mit Alt und die Funktionstasten jedoch stets vollständig zur Verfügung stehen.

3.3 YaST-Kommandozeilenoptionen

Neben der Schnittstelle im Textmodus bietet YaST auch eine reine Kommandozeilenschnittstelle. Eine Liste der YaST-Kommandozeilenoptionen erhalten Sie, wenn Sie Folgendes eingeben:

```
yast -h
```

3.3.1 Starten der einzelnen Module

Um Zeit zu sparen können die einzelnen YaST-Module direkt gestartet werden. Um ein Modul zu starten, geben Sie Folgendes ein:

```
yast <module_name>
```

Eine Liste aller auf Ihrem System verfügbaren Modulnamen können Sie mit `yast -l` oder `yast --list` anzeigen. Das Netzwerkmodul beispielsweise wird mit `yast lan` gestartet.

3.3.2 Installation von Paketen über die Kommandozeile

Wenn Sie den Namen eines Pakets kennen und das Paket von einer Ihrer aktiven Installations-Repositorys bereitgestellt wird, können Sie das Paket mithilfe der Kommandozeilenoption `-i` installieren.

```
yast -i <package_name>
```

oder

```
yast --install <package_name>
```

package_name kann ein einzelner kurzer Paketname sein, beispielsweise `gvim` (solche Pakete werden mit Abhängigkeitsüberprüfung installiert) oder der vollständige Pfad zu einem RPM-Paket, das ohne Abhängigkeitsüberprüfung installiert wird.

Wenn Sie ein kommandozeilenbasiertes Softwareverwaltungs-Dienstprogramm mit Funktionen benötigen, die über die von YaST hinausgehen, sollten Sie möglicherweise zypper verwenden. Dieses neue Dienstprogramm verwendet die Softwareverwaltungsbibliothek, die auch die Grundlage des YaST-Paket-Managers bildet. Die grundlegende Verwendung von Zypper wird in Abschnitt 7.1, „Verwenden von zypper“ (S. 73) erläutert.

3.3.3 Kommandozeilenparameter der YaST-Module

Um die Verwendung von YaST-Funktionen in Skripts zu ermöglichen, bietet YaST Kommandozeilenunterstützung für einzelne Module. Die Kommandozeilenunterstützung steht jedoch nicht für alle Module zur Verfügung. Um die verfügbaren Optionen eines Moduls anzuzeigen, geben Sie Folgendes ein:

```
yast <module_name> help
```

Wenn ein Modul keine Kommandozeilenunterstützung bietet, wird es im Textmodus gestartet und es wird folgende Meldung angezeigt.

```
This YaST module does not support the command line interface.
```



Snapshots/Rollback mit Snapper

4

Viele Benutzer fragten bereits nach einer Funktion, mit der sie Snapshots des Dateisystems anfertigen könnten, um so Rollbacks für Linux auszuführen. Dank Snapper, gemeinsam mit dem `Btrfs`-Dateisystem oder mit Thin Provisioned LVM-Volumes, ist diese Lücke nunmehr geschlossen.

Das neue Copy-on-Write-Dateisystem `Btrfs` für Linux unterstützt Dateisystem-Snapshots (Kopie des Zustands eines Subvolume zu einem bestimmten Zeitpunkt) von Subvolumes (ein oder mehrere separat einhängbare Dateisysteme auf den einzelnen physischen Partitionen). Mit Snapper verwalten Sie diese Snapshots. Snapper ist mit einer Kommandozeile und einer YaST-Oberfläche ausgestattet.

Standardmäßig fungieren Snapper und `Btrfs` unter SUSE Linux Enterprise Desktop als „Rückgängig-Werkzeug" bei Systemänderungen, die mit YaST oder zypper durchgeführt wurden. Vor und nach dem Ausführen eines YaST-Moduls oder von zypper wird ein Snapshot erstellt. Mit Snapper können Sie die beiden Snapshots vergleichen, und Sie erhalten die Möglichkeit, die Unterschiede zwischen den beiden Snapshots wieder rückgängig zu machen. Die Werkzeuge sorgen außerdem für die Systemsicherung, da stündlich ein Snapshot der System-Subvolumes angefertigt wird.

4.1 Anforderungen

`Btrfs` bietet als einziges Dateisystem unter SUSE Linux Enterprise Desktop die Unterstützung für Snapshots und ist daher auf allen Partitionen und Subvolumes erforderlich, für die ein „Snapshot" angefertigt werden soll.

4.1.1 Snapshots und Festplattenspeicher

Beim Erstellen eines Snapshots verweisen sowohl der Snapshot als auch das Original auf dieselben Blöcke im Dateisystem. Zunächst belegt ein Snapshot also keinen zusätzlichen Speicherplatz auf der Festplatte. Werden Daten im Original-Dateisystem bearbeitet, so werden die geänderten Datenblöcke kopiert, und die alten Datenblöcke werden im Snapshot beibehalten. Der Snapshot belegt daher dieselbe Speicherplatzmenge wie die geänderten Daten. Im Lauf der Zeit wächst der Speicherplatzbedarf eines Snapshots somit an. Wenn Sie also Dateien aus einem `Btrfs`-Dateisystem löschen, auf dem sich Snapshots befinden, wird unter Umständen *kein* Speicherplatz freigegeben!

ANMERKUNG: Position der Snapshots

Snapshots befinden sich stets auf derselben Partition oder demselben Subvolume wie die Daten, für die der „Snapshot" angefertigt wurde. Es ist nicht möglich, einen Snapshot auf einer anderen Partition oder einem anderen Subvolume zu speichern.

Partitionen mit Snapshots müssen daher größer sein als „normale" Partitionen. Die Speichermenge ist dabei abhängig von der Anzahl der Snapshots und vom Umfang der Änderungen an den Daten. In der Regel sollten Sie etwa den doppelten Speicherplatz bereitstellen.

TIPP: Freigeben von Speicherplatz/Belegung des Festplattenspeichers

Um Speicherplatz auf einer `Btrfs`-Partition mit Snapshots freizugeben, müssen Sie keine Dateien löschen, sondern die nicht mehr benötigten Snapshots. Ältere Snapshots belegen mehr Speicherplatz als neuere Snapshots.

Da das Kommando `df` nicht die richtige Menge an belegtem Speicherplatz auf `Btrfs`-Dateisystemen angibt, müssen Sie das Kommando `btrfs filesystem df` *`MOUNT_POINT`* verwenden. Die `Btrfs`-Werkzeuge unterstützen zurzeit noch nicht die Anzeige des Speicherplatzes, der von einem Snapshot belegt wird.

Wenn Sie eine Aufrüstung von einem Service Pack auf ein höheres Service Pack vornehmen, belegen die entstehenden Snapshots einen großen Teil des Festplattenspeichers auf den System-Subvolumes, da große Mengen an Daten

geändert werden (Aktualisierungen der Pakete). Es wird daher empfohlen, diese Snapshots manuell zu löschen, sobald Sie sie nicht mehr benötigen.

Mit Snapper können Sie außerdem Snapshots auf Thin Provisioned LVM-Volumes, die mit ext3 oder XFS formatiert sind, erstellen und verwalten (siehe Abschnitt 4.6, „Verwenden von Snapper auf Thin Provisioned LVM-Volumes“ (S. 52)).

4.2 Rückgängigmachen von Systemänderungen mit Snapper

Snapper unter SUSE Linux Enterprise Desktop ist als Werkzeug vorkonfiguriert, mit dem Sie die Änderungen rückgängig machen, die von `zypper` und YaST vorgenommen werden. Hierzu ist Snapper so konfiguriert, dass vor und nach jeder Ausführung von `zypper` bzw. YaST ein Snapshot-Paar erstellt wird. Mit Snapper können Sie außerdem Systemdateien wiederherstellen, die versehentlich gelöscht oder geändert wurden. Hierzu werden stündliche Sicherungen angelegt.

Standardmäßig werden automatische Snapshots (wie oben beschrieben) für die Root-Partition und deren Subvolumes konfiguriert. Sollen Snapshots auch für andere Partitionen zur Verfügung stehen, beispielsweise für `/home`, können Sie benutzerdefinierte Konfigurationen anlegen.

4.2.1 Rückgängigmachen von Änderungen durch YaST oder Zypper

Wenn Sie die Root-Partition während der Installation mit `Btrfs` einrichten, wird Snapper (für Rollbacks von Änderungen durch YaST oder Zypper vorkonfiguriert) automatisch installiert. Bei jedem Starten eines YaST-Moduls und bei jeder Zypper-Transaktion werden zwei Snapshots erstellt: ein „Pre-Snapshot“ mit dem Zustand des Dateisystems vor dem Start des Moduls und ein „Post-Snapshot“ nach Beendigung des Moduls.

Mit dem YaST-Snapper-Modul oder mit dem `snapper`-Kommandozeilenwerkzeug können Sie Dateien aus dem „Pre-Snapshot“ wiederherstellen und so die Änderungen durch YaST/Zypper rückgängig machen. Durch den Vergleich der beiden Snapshots

mit diesen Werkzeugen erkennen Sie außerdem, welche Dateien geändert wurden. Darüber hinaus können Sie die Unterschiede (Diff) zwischen zwei Versionen einer Datei abrufen.

Linux ist ein Multitasking-System, weshalb die Daten im Zeitraum zwischen dem Pre-Snapshot und dem Post-Snapshot durchaus auch durch andere Prozesse (außer YaST und zypper) geändert werden können. In diesem Fall werden auch alle Änderungen durch andere Prozesse rückgängig gemacht, wenn Sie den Zustand aus dem Pre-Snapshot wiederherstellen. In der Regel ist dies eher unerwünscht. Überprüfen Sie daher sorgfältig alle Änderungen zwischen den beiden Snapshots, bevor Sie das Rollback starten. Wenn Sie Änderungen aus anderen Prozessen finden, die beibehalten werden sollen, wählen Sie die Dateien für das Rollback aus.

WICHTIG: Einschränkungen

Machen Sie sich mit den Einschränkungen von Snapper vertraut, bevor Sie die Rollback-Funktion nutzen. Weitere Informationen finden Sie in Abschnitt 4.4, „Einschränkungen“ (S. 50).

ANMERKUNG: Speicherdauer der Snapshots

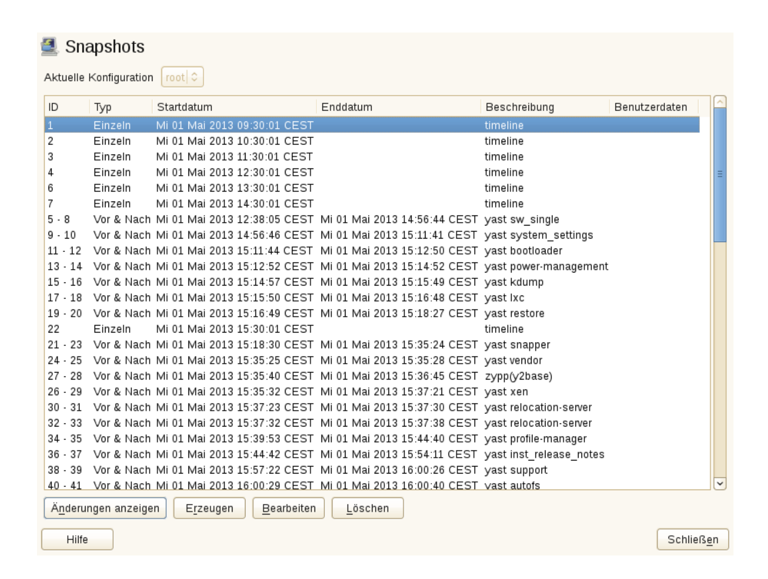
Standardmäßig werden die letzten 100 YaST- und zypper-Snapshots beibehalten. Sobald diese Anzahl überschritten wird, werden die ältesten Snapshots gelöscht.

Prozedur 4.1 *Rückgängigmachen von Änderungen mit dem Snapper-Modul in YaST*

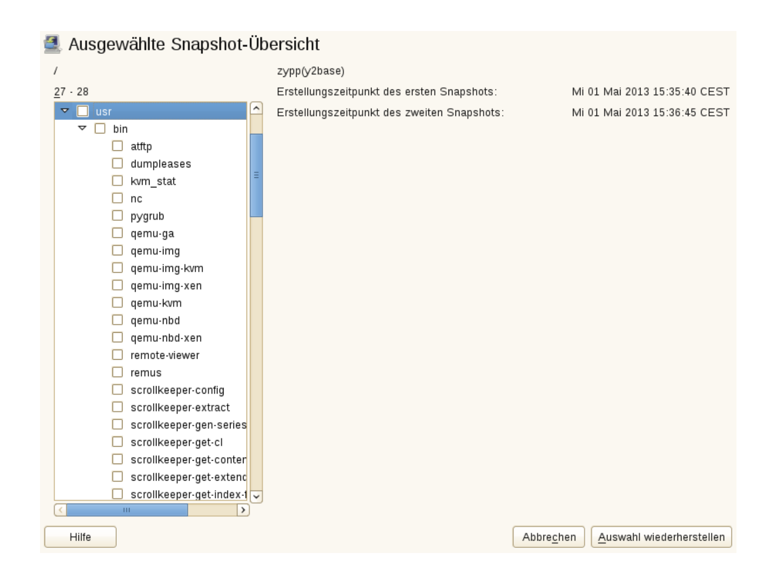
1. Starten Sie das *Snapper*-Modul im Abschnitt *Verschiedenes* in YaST, oder geben Sie `yast2 snapper` ein.

2. Unter *Aktuelle Konfiguration* muss die Option *root* eingestellt sein. Dies ist im Prinzip immer der Fall, sofern Sie nicht eigene Snapper-Konfigurationen manuell hinzugefügt haben.

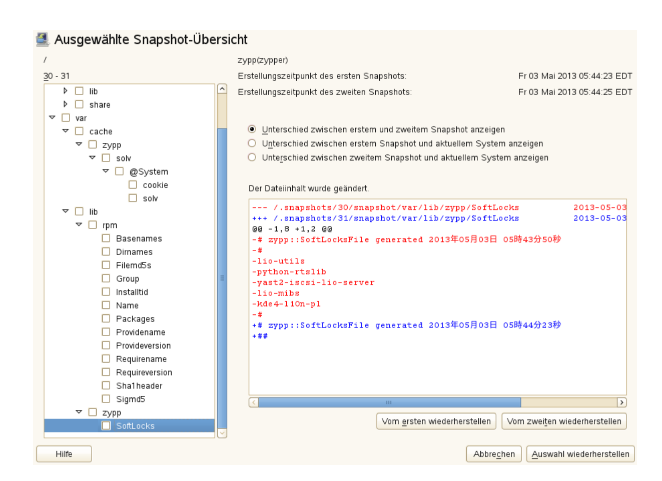
3. Wählen Sie ein Pre-/Post-Snapshot-Paar aus der Liste aus. Sowohl die YaST als auch die Zypper-Snapshot-Paare sind vom Typ *Pre & Post*. Für YaST-Snapshots wird die Bezeichnung `yast` *`Modulname`* in der *Spalte „Beschreibung“* angezeigt, für zypper-Snapshots die Bezeichnung `zypp(zypper)`.



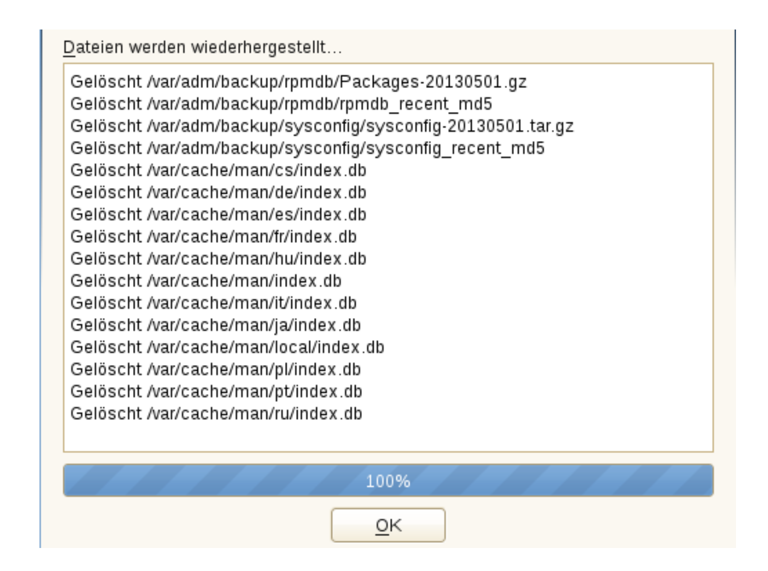
4 Klicken Sie auf *Änderungen anzeigen*. Die Liste der Dateien, bei denen Unterschiede zwischen den beiden Snapshots bestehen, wird geöffnet. Die nachfolgende Abbildung zeigt eine Liste von Dateien, die nach dem Hinzufügen des Benutzers `tester` geändert wurden.



5 Prüfen Sie die Dateiliste. Zum Anzeigen der Unterschiede („Diff“) zwischen der Pre- und der Post-Version einer Datei wählen Sie die Datei aus der Liste aus. Die nachfolgenden Abbildungen zeigen die Änderungen an der Datei `/etc/passwd`, die nach dem Hinzufügen des Benutzers `tester` vorgenommen wurden.



6 Zum Wiederherstellen einer Reihe von Dateien aktivieren Sie das entsprechende Kontrollkästchen für die gewünschten Dateien oder Verzeichnisse. Klicken Sie auf *Auswahl wiederherstellen*, und bestätigen Sie den Vorgang mit *Ja*.



Zum Wiederherstellen einer einzelnen Datei klicken Sie auf den Namen dieser Datei. Die Diff-Ansicht der Datei wird aktiviert. Klicken Sie auf *Vom ersten wiederherstellen*, und bestätigen Sie mit *Ja*.

Prozedur 4.2 *Rückgängigmachen von Änderungen mit dem Kommando snapper*

1 Mit dem Kommando `snapper list -t pre-post` erhalten Sie eine Liste der YaST- und zypper-Snapshots. Für YaST-Snapshots wird die Bezeichnung `yast Modulname` in der *Spalte „Beschreibung“* angezeigt, für zypper-Snapshots die Bezeichnung `zypp(zypper)`.

```
~ # snapper list -t pre-post
    Pre # | Post # | Pre Date                 | Post Date                | Description

------+--------+--------------------------+--------------------------+----------------------+

    4     | 5      | Tue Jan 10 14:39:14 2012 | Tue Jan 10 14:39:33 2012 | yast system_settings

    65    | 66     | Thu Jan 12 17:18:10 2012 | Thu Jan 12 17:18:23 2012 | zypp(zypper)
    68    | 69     | Thu Jan 12 17:25:46 2012 | Thu Jan 12 17:27:09 2012 | zypp(zypper)
    73    | 74     | Thu Jan 12 17:32:55 2012 | Thu Jan 12 17:33:13 2012 | yast system_settings

    75    | 76     | Thu Jan 12 17:33:56 2012 | Thu Jan 12 17:34:42 2012 | yast users
    77    | 92     | Thu Jan 12 17:38:36 2012 | Thu Jan 12 23:13:13 2012 | yast snapper
    83    | 84     | Thu Jan 12 22:10:33 2012 | Thu Jan 12 22:10:39 2012 | zypp(zypper)
    85    | 86     | Thu Jan 12 22:16:58 2012 | Thu Jan 12 22:17:09 2012 | zypp(zypper)
    88    | 89     | Thu Jan 12 23:10:42 2012 | Thu Jan 12 23:10:46 2012 | zypp(zypper)
    90    | 91     | Thu Jan 12 23:11:40 2012 | Thu Jan 12 23:11:42 2012 | zypp(zypper)
    108   | 109    | Fri Jan 13 13:01:06 2012 | Fri Jan 13 13:01:10 2012 | zypp(zypper)
```

2 Mit dem Kommando `snapper status PRE erhalten Sie eine Liste der geänderten Dateien für ein Snapshot-Paar.POST`. Dateien, deren Inhalt geändert wurde, sind mit *c* gekennzeichnet, hinzugefügte Dateien mit + und gelöschte Dateien mit -. Das nachfolgende Beispiel zeigt ein Snapshot-Paar für die Installation des Pakets `ncftp`.

```
~ # snapper status 108..109
     +... /usr/bin/ncftp
     +... /usr/bin/ncftpbatch
     +... /usr/bin/ncftpget
     +... /usr/bin/ncftpls
     [...]
     +... /usr/share/man/man1/ncftpspooler.1.gz
     c... /var/cache/zypp/solv/@System/cookie
     c... /var/cache/zypp/solv/@System/solv
     c... /var/lib/rpm/Basenames
     c... /var/lib/rpm/Dirnames
     c... /var/lib/rpm/Filemd5s
```

```
c... /var/lib/rpm/Group
c... /var/lib/rpm/Installtid
c... /var/lib/rpm/Name
c... /var/lib/rpm/Packages
c... /var/lib/rpm/Providename
c... /var/lib/rpm/Provideversion
c... /var/lib/rpm/Requirename
c... /var/lib/rpm/Requireversion
c... /var/lib/rpm/Sha1header
c... /var/lib/rpm/Sigmd5
c... /var/lib/zypp/SoftLocks
```

3 Zum Anzeigen der Unterschiede (Diff) für eine bestimmte Datei führen Sie `snapper diff` *`PRE`* `aus.`*`POST FILENAME`*. Wenn Sie *`FILENAME`* nicht angeben, wird die Diff-Ansicht für alle Dateien angezeigt.

```
~ # snapper diff 108..109 /var/lib/zypp/SoftLocks
     --- /.snapshots/108/snapshot/var/lib/zypp/SoftLocks 2012-01-12
23:15:22.408009164 +0100
     +++ /.snapshots/109/snapshot/var/lib/zypp/SoftLocks 2012-01-13
13:01:08.724009131 +0100
     @@ -1,4 +1,2 @@
     -# zypp::SoftLocksFile generated Thu Jan 12 23:10:46 2012
     -#
     -ncftp
     -#
     +# zypp::SoftLocksFile generated Fri Jan 13 13:01:08 2012
     +##
```

4 Zum Wiederherstellen einer oder mehrerer Dateien führen Sie `snapper -v undochange` *`PRE`* `aus.`*`POST FILENAMES`*. Wenn Sie *`FILENAMES`* nicht angeben, werden alle geänderten Dateien wiederhergestellt.

```
~ # snapper -v undochange 108..109
     create:0 modify:16 delete:21
     undoing change...
     deleting /usr/share/man/man1/ncftpspooler.1.gz
     deleting /usr/share/man/man1/ncftpput.1.gz
     [...]
     deleting /usr/bin/ncftpls
     deleting /usr/bin/ncftpget
     deleting /usr/bin/ncftpbatch
     deleting /usr/bin/ncftp
     modifying /var/cache/zypp/solv/@System/cookie
     modifying /var/cache/zypp/solv/@System/solv
     modifying /var/lib/rpm/Basenames
     modifying /var/lib/rpm/Dirnames
     modifying /var/lib/rpm/Filemd5s
     modifying /var/lib/rpm/Group
     modifying /var/lib/rpm/Installtid
```

```
modifying /var/lib/rpm/Name
modifying /var/lib/rpm/Packages
modifying /var/lib/rpm/Providename
modifying /var/lib/rpm/Provideversion
modifying /var/lib/rpm/Requirename
modifying /var/lib/rpm/Requireversion
modifying /var/lib/rpm/Sha1header
modifying /var/lib/rpm/Sigmd5
modifying /var/lib/zypp/SoftLocks
undoing change done
```

4.2.2 Wiederherstellen von Dateien aus stündlichen Sicherungen mit Snapper

Neben den YaST- und zypper-Snapshots erstellt Snapper stündliche Snapshots der Systempartition (`/`). Mit diesen Sicherungs-Snapshots können Sie Dateien wiederherstellen, die versehentlich gelöscht oder geändert wurden. Mit der Diff-Funktion in Snapper können Sie außerdem feststellen, welche Änderungen an einem bestimmten Zeitpunkt vorgenommen wurden.

Die stündlichen Sicherungs-Snapshots sind vom Typ `Einzeln` und tragen die Bezeichnung `Zeitleiste`. Zum Wiederherstellen von Dateien aus diesen Snapshots befolgen Sie die Anweisungen unter Prozedur 4.1, „Rückgängigmachen von Änderungen mit dem *Snapper*-Modul in YaST“ (S. 34) oder Prozedur 4.2, „Rückgängigmachen von Änderungen mit dem Kommando `snapper`“ (S. 37).

ANMERKUNG: Speicherdauer der Snapshots

Standardmäßig wird der erste Snapshot der letzten zehn Tage, Monate und Jahre beibehalten. Weitere Informationen finden Sie unter Beispiel 4.1, „Beispiel für eine Zeitleistenkonfiguration“ (S. 42).

4.2.3 Erstellen und Bearbeiten von Snapper-Konfigurationen

Das Verhalten von Snapper ist in je einer Konfigurationsdatei pro Partition und `Btrfs`-Subvolume definiert. Diese Konfigurationsdateien sind unter `/etc/snapper/configs/` gespeichert. Die Standardkonfiguration in Snapper für das Verzeichnis `/`

trägt die Bezeichnung root. Hiermit werden die YaST- und Zypper-Snapshots sowie die stündlichen Sicherungs-Snapshots für / erstellt und verwaltet.

Sie können eigene Konfigurationen für andere, mit Btrfs formatierte Partitionen sowie für vorhandene Subvolumes auf einer Btrfs-Partition erstellen. Im nachfolgenden Beispiel wird eine Snapper-Konfiguration zum Sichern der Webserverdaten eingerichtet, die sich auf einer separaten, mit Btrfs formatierten, unter /srv/www eingehängten Partition befinden.

Zum Wiederherstellen von Dateien aus diesen Snapshots verwenden Sie wahlweise snapper selbst oder das *Snapper*-Modul in YaST. In YaST wählen Sie die *Aktuelle Konfiguration* aus, wobei Sie die Konfiguration für snapper mit dem globalen Schalter -c angeben (z. B. snapper -c myconfig list).

Zum Erstellen einer neuen Snapper-Konfiguration führen Sie snapper create-config aus:

```
snapper -c www-data❶ create-config
   /srv/www❷
```

❶ Der Name der Konfigurationsdatei.

❷ Einhängepunkt für die Partition oder das Btrfs-Subvolume am Snapshot.

Mit diesem Kommando erstellen Sie eine neue Konfigurationsdsdatei /etc/snapper/config-templates/www-data mit geeigneten Standardwerten (aus /etc/snapper/config-templates/default übernommen).

TIPP: Standardwerte für die Konfiguration

Die Standardwerte für eine neue Konfiguration werden aus /etc/snapper/config-templates/default übernommen. Sollen eigene Standardwerte verwendet werden, erstellen Sie eine Kopie dieser Datei in demselben Verzeichnis, und passen Sie diese Kopie gemäß Ihren Anforderungen an. Geben Sie dann die Option -t option für das Kommando create-config an:

```
snapper -c www-data create-config -t my_defaults /srv/www
```

4.2.3.1 Anpassen der Konfigurationsdatei

Die Konfigurationsdatei lässt sich in einem Editor bearbeiten. Hier befinden sich Schlüssel-Wert-Paare im Format `Schlüssel=Wert`. Sie können lediglich den `Wert` bearbeiten.

`SUBVOLUME`
: Einhängepunkt für die Partition oder das Subvolume am Snapshot. Bearbeiten Sie diese Datei nicht.

`FSTYPE`
: Dateisystemtyp der Partition. Bearbeiten Sie diese Datei nicht.

`NUMBER_CLEANUP`
: Legt fest, ob alte Snapshots automatisch gelöscht werden sollen, sobald die mit `NUMBER_LIMIT` angegebene Anzahl *und* das mit `NUMBER_MIN_AGE` angegebene Alter erreicht werden. Gültige Werte: `yes`, `no`

> **ANMERKUNG: Grenzwert und Alter**
>
> `NUMBER_LIMIT` und `NUMBER_MIN_AGE` werden stets gemeinsam ausgewertet. Die Snapshots werden nur dann gelöscht, wenn *beide* Bedingungen erfüllt sind. Wenn stets eine bestimmte Anzahl von Snapshots unabhängig von ihrem Alter beibehalten werden soll, setzen Sie `NUMBER_MIN_AGE` auf `0`. Sollen umgekehrt Snapshots nicht über ein bestimmtes Alter hinaus beibehalten werden, setzen Sie `NUMBER_LIMIT` auf `0`.

`NUMBER_LIMIT`
: Definiert die Anzahl der beizubehaltenden Snapshots, wenn `NUMBER_CLEANUP` auf `yes` gesetzt ist.

`NUMBER_MIN_AGE`
: Definiert das Mindestalter in Sekunden, das ein Snapshot aufweisen soll, bevor er automatisch gelöscht werden kann.

`TIMELINE_CREATE`
: Wenn diese Option auf `yes` gesetzt ist, werden stündliche Snapshots erstellt. Dies ist zurzeit die einzige Möglichkeit, um Snapshots automatisch zu erstellen. Die Einstellung `yes` wird daher dringend empfohlen. Gültige Werte: `yes`, `no`

`TIMELINE_CLEANUP`
: Legt fest, ob alte Snapshots automatisch gelöscht werden sollen, sobald die mit *`TIMELINE_LIMIT_*`* angegebene Anzahl *und* das mit `TIMELINE_MIN_AGE` angegebene Alter erreicht werden. Gültige Werte: `yes`, `no`

`TIMELINE_MIN_AGE`
: Definiert das Mindestalter in Sekunden, das ein Snapshot aufweisen soll, bevor er automatisch gelöscht werden kann.

`TIMELINE_LIMIT_HOURLY`, `TIMELINE_LIMIT_DAILY`, `TIMELINE_LIMIT_MONTHLY`, `TIMELINE_LIMIT_YEARLY`
: Anzahl der Snapshots, die pro Stunde, Tag, Monat und Jahr beibehalten werden sollen.

Beispiel 4.1 *Beispiel für eine Zeitleistenkonfiguration*

```
TIMELINE_CREATE="yes"
        TIMELINE_CLEANUP="yes"
        TIMELINE_MIN_AGE="1800"
        TIMELINE_LIMIT_HOURLY="10"
        TIMELINE_LIMIT_DAILY="10"
        TIMELINE_LIMIT_MONTHLY="10"
        TIMELINE_LIMIT_YEARLY="10"
```

In dieser Beispielkonfiguration werden stündliche Snapshots vorgenommen, die automatisch bereinigt werden. `TIMELINE_MIN_AGE` und `TIMELINE_LIMIT_*` werden stets gemeinsam ausgewertet. In diesem Beispiel ist das Mindestalter eines Snapshots, ab dem er gelöscht werden kann, auf 30 Minuten (1800 Sekunden) eingestellt. Durch die stündliche Erstellung der Snapshots werden nur die jeweils neuesten Snapshots beibehalten. Wenn `TIMELINE_LIMIT_DAILY` auf einen Wert ungleich null gesetzt ist, wid auch der erste Snapshot des Tages beibehalten.

Beizubehaltende Snapshots

- Stündlich: Die letzten zehn angefertigten Snapshots.
- Täglich: Jeweils der erste Snapshot, der zu Tagesbeginn angefertigt wurde, für die letzten zehn Tage.
- Monatlich: Jeweils der erste Snapshot, der am letzten Tag des Monats angefertigt wurde, für die letzten zehn Monate.

- Jährlich: Jeweils der erste Snapshot, der am letzten Tag des Jahres angefertigt wurde, für die letzten zehn Jahre.

4.2.3.2 Verwenden von Snapper als normaler Benutzer

Standardmäßig kann Snapper nur von `root` verwendet werden. Unter Umständen müssen jedoch bestimmte Gruppen oder Benutzer in der Lage sein, Snapshots zu erstellen oder Änderungen durch Wiederherstellen eines Snapshots rückgängig zu machen:

- Ein Website-Administrator möchte einen Snapshot von `/srv/www` anfertigen.
- Ein Datenbankadministrator möchte einen Snapshot der Datenbanken anfertigen.
- Eine Benutzerin möchte einen Snapshot ihres Benutzerverzeichnisses anfertigen.

Für diese Zwecke können Sie Snapper-Konfigurationen erstellen, in denen Benutzern und/oder Gruppen Berechtigungen gewährt werden. Neben dieser Konfigurationsänderung muss das zugehörige Verzeichnis `.snapshots` für die jeweiligen Benutzer lesbar und zugänglich sein.

Prozedur 4.3 *Ermöglichen der Verwendung von Snapper für normale Benutzer*

Beachten Sie, dass alle Schritte in diesem Verfahren von `root` ausgeführt werden müssen.

1 Erstellen Sie eine Snapper-Konfiguration für die Partition oder das Subvolume, auf dem der Benutzer Snapper verwenden soll (falls noch nicht vorhanden). Weitere Anweisungen finden Sie unter Abschnitt 4.2.3, „Erstellen und Bearbeiten von Snapper-Konfigurationen“ (S. 39). Beispiel:

```
snapper --config web_data create /srv/www
```

2 Die Konfigurationsdatei wird unter `/etc/snapper/configs/NAME` angelegt, wobei NAME dem Wert entspricht, den Sie im vorherigen Schritt mit `-c/--config` angegeben haben (beispielsweise `/etc/snapper/configs/webdaten`). Nehmen Sie die gewünschten Anpassungen vor (Details finden Sie unter Abschnitt 4.2.3.1, „Anpassen der Konfigurationsdatei“ (S. 41)).

3 Legen Sie Werte für ALLOW_USERS und/oder ALLOW_GROUPS fest. Damit gewähren Sie bestimmten Benutzern bzw. Gruppen die Berechtigungen. Mehrere Einträge müssen mit Leertaste getrennt werden. Um beispielsweise dem Benutzer www_admin Berechtigungen zu gewähren, geben Sie Folgendes ein:

```
ALLOW_USERS="www_admin"
```

4 Gewähren Sie Lese- und Zugriffsberechtigungen für das Snapshot-Verzeichnis *PATH*/.snapshots. *PATH* muss dabei durch das Subvolume ersetzt werden, das Sie im ersten Schritt dieses Verfahrens angegeben haben. Beispiel:

```
chmod a+rx /srv/www/.snapshots
```

Die vorhandene Snapper-Konfiguration kann nunmehr durch den oder die angegebenen Benutzer und/oder Gruppen verwendet werden. Testen Sie dies beispielsweise mit dem Kommando list:

```
www_admin:~ > snapper -c web_data list
```

4.2.4 Deaktivieren der automatischen Snapshots

Wenn Sie die Root-Partition während der Installation mit Btrfs eingerichtet haben, erstellt Snapper automatisch stündliche Snapshots des Systems sowie Pre- und Post-Snapshots bei YaST- und zypper-Transaktionen. Diese Aufgaben lassen sich jeweils wie folgt deaktivieren:

Deaktivieren der stündlichen Snapshots
: Bearbeiten Sie /etc/snapper/configs/root, und setzen Sie TIMELINE_CREATE auf no:

```
TIMELINE_CREATE="no"
```

Deaktivieren der zypper-Snapshots
: Deinstallieren Sie das Paket snapper-zypp-plugin

Deaktivieren der YaST-Snapshots
: Bearbeiten Sie /etc/sysconfig/yast2, und setzen Sie USE_SNAPPER auf no:

```
USE_SNAPPER="no"
```

4.3 Manuelles Erstellen und Verwalten von Snapshots

Snapper ist nicht auf das automatische Erstellen und Verwalten von Snapshots über eine Konfiguration beschränkt. Mit dem Kommandozeilenwerkzeug oder dem YaST-Modul können Sie auch selbst Snapshot-Paare („vorher/nachher“) oder einzelne Snapshots manuell erstellen.

Alle Snapper-Vorgänge werden für eine vorhandene Konfiguration ausgeführt (weitere Details finden Sie unter Abschnitt 4.2.3, „Erstellen und Bearbeiten von Snapper-Konfigurationen“ (S. 39)). Sie können einen Snapshot nur für Partitionen oder Volumes erstellen, für die eine Konfiguration vorhanden ist. Standardmäßig wird die Systemkonfiguration (`root`) verwendet. Wenn Sie Snapshots für Ihre eigene Konfiguration erstellen oder verwalten möchten, müssen Sie diese Konfiguration explizit auswählen. Verwenden Sie das Dropdown-Menü *Aktuelle Konfiguration* in YaST, oder geben Sie den Schalter `-c` in der Kommandozeile an (`snapper -c` *`MYCONFIG COMMAND`*).

4.3.1 Snapshot-Metadaten

Ein Snapshot besteht jeweils aus dem Snapshot selbst und aus einigen Metadaten. Beim Erstellen eines Snapshots müssen Sie auch die Metadaten angeben. Wenn Sie einen Snapshot bearbeiten, so ändern Sie die Metadaten – der Inhalt selbst kann nicht bearbeitet werden. Die folgenden Metadaten sind für jeden Snapshot verfügbar:

- **Typ**: Snapshot-Typ; Details siehe Abschnitt 4.3.1.1, „Snapshot-Typen“ (S. 46). Diese Daten können nicht geändert werden.

- **Nummer:** Eindeutige Nummer des Snapshots. Diese Daten können nicht geändert werden.

- **Pre Number (Pre-Nummer):** Nummer des zugehörigen Pre-Snapshots. Nur für Snapshots vom Post-Typ. Diese Daten können nicht geändert werden.

- **Beschreibung:** Beschreibung des Snapshots.

- **Benutzerdaten:** Erweiterte Beschreibung, in der Sie benutzerdefinierte Daten als kommagetrennte Liste im Format Schlüssel=Wert angeben können, beispielsweise `reason=testing_stuff, user=&tux`

- **Bereinigungsalgorithmus**: Bereinigungsalgorithmus für den Snapshot; Details siehe Abschnitt 4.3.1.2, „Bereinigungsalgorithmen“ (S. 46).

4.3.1.1 Snapshot-Typen

In Snapper gibt es drei Typen von Snapshots: pre, post und einzeln. Physisch unterscheiden sie sich nicht, sie werden jedoch in Snapper unterschiedlich behandelt.

`Pre`
: Snapshot eines Dateisystems *vor* einer Änderung. Zu jedem `Pre`-Snapshot gibt es einen zugehörigen `Post`-Snapshot. Wird beispielsweise für die automatischen YaST-/zypper-Snapshots verwendet.

`Post`
: Snapshot eines Dateisystems *nach* einer Änderung. Zu jedem `Post`-Snapshot gibt es einen zugehörigen `Pre`-Snapshot. Wird beispielsweise für die automatischen YaST-/zypper-Snapshots verwendet.

`Einzeln`
: Eigenständiger Snapshot. Wird beispielsweise für die automatischen stündlichen Snapshots verwendet. Dies ist der Standardtyp beim Erstellen von Snapshots.

4.3.1.2 Bereinigungsalgorithmen

Snapper bietet drei Algorithmen zum Bereinigen alter Snapshots. Die Algorithmen werden im Rahmen eines täglichen CRON-Auftrags ausgeführt. Die Bereinigungshäufigkeit selbst ist in der Snapper-Konfiguration für die Partition oder das Subvolume definiert (weitere Informationen siehe Abschnitt 4.2.3.1, „Anpassen der Konfigurationsdatei“ (S. 41)).

Zahl
: Löscht alte Snapshots, sobald eine bestimmte Anzahl von Snapshots erreicht wird.

Zeitleiste
: Löscht Snapshots, die ein bestimmtes Alter erreicht haben; hierbei wird allerdings eine Reihe von stündlichen, täglichen, monatlichen und jährlichen Snapshots beibehalten.

empty-pre-post (Leer-Pre-Post)
: Löscht Pre-/Post-Snapshot-Paare, zwischen denen keine Unterschiede (Diffs) bestehen.

4.3.2 Erstellen von Snapshots

Zum Erstellen eines Snapshots führen Sie `snapper create` aus, oder klicken Sie im *Snapper*-Modul in YaST auf *Erstellen*. In den nachfolgenden Beispielen wird erläutert, wie Sie Snapshots über die Kommandozeile erstellen. Die Anpassung ist über die YaST-Oberfläche ganz einfach.

TIPP: Snapshot-Beschreibung

Geben Sie stets eine aussagekräftige Beschreibung an, mit der der Zweck des Snapshots auch später noch eindeutig erkennbar ist. Über die Option für die Benutzerdaten können Sie noch mehr Informationen festlegen.

`snapper create --description "Snapshot für Woche 2 2013"`
: Erstellt einen eigenständigen Snapshot (Einzeltyp) für die Standardkonfiguration (`root`) mit einer Beschreibung. Da kein Bereinigungsalgorithmus angegeben ist, wird der Snapshot nicht automatisch gelöscht.

`snapper --config home create --description "Bereinigung in ~tux"`
: Erstellt einen eigenständigen Snapshot (Einzeltyp) für die benutzerdefinierte Konfiguration (`home`) mit einer Beschreibung. Da kein Bereinigungsalgorithmus angegeben ist, wird der Snapshot nicht automatisch gelöscht.

`snapper --config home create --description "Tägliche Datensicherung" --cleanup-algorithm timeline`
: Erstellt einen eigenständigen Snapshot (Einzeltyp) für die benutzerdefinierte Konfiguration (`home`) mit einer Beschreibung. Die Datei wird automatisch gelöscht,

sobald die Kriterien für den Zeitleisten-Bereinigungsalgorithmus in der Konfiguration erfüllt sind.

`snapper create --type pre--print-number--description "Vor Apache-Konfigurationsbereinigung"`
: Erstellt einen Snapshot vom `Pre`-Typ und gibt die Snapshot-Nummer aus. Erstes Kommando zum Erstellen eines Snapshot-Paars, mit dem der „Vorher“-/„Nachher“-Zustand festgehalten wird.

`snapper create --type post--pre-number 30--description "Nach der Apache-Konfigurationsbereinigung"`
: Erstellt einen Snapshot vom `Post`-Typ, gepaart mit der `Pre`-Snapshot-Nummer `30`. Zweites Kommando zum Erstellen eines Snapshot-Paars, mit dem der „Vorher“-/„Nachher“-Zustand festgehalten wird.

`snapper create --command` *`COMMAND`*`--description "Vor und nach KOMMANDO"`
: Erstellt automatisch ein Snapshot-Paar vor und nach dem Ausführen von *`KOMMANDO`*. Diese Option ist nur verfügbar, wenn Snapper in der Kommandozeile verwendet wird.

4.3.3 Bearbeiten von Snapshot-Metadaten

Bei Snapper können Sie die Beschreibung, den Bereinigungsalgorithmus und die Metadaten eines Snapshots bearbeiten. Alle anderen Metadaten können nicht geändert werden. In den nachfolgenden Beispielen wird erläutert, wie Sie Snapshots über die Kommandozeile bearbeiten. Die Anpassung ist über die YaST-Oberfläche ganz einfach.

Um einen Snapshot in der Kommandozeile zu bearbeiten, müssen Sie seine Nummer kennen. Mit `snapper list` rufen SIe alle Snapshots mit den dazugehörigen Nummern ab.

Im *Snapper*-Modul in YaST werden bereits alle Snapshots aufgelistet. Wählen Sie einen Eintrag in der Liste, und klicken Sie auf *Bearbeiten*.

`snapper modify --cleanup-algorithm "Zeitleiste" 10`
: Bearbeitet die Metadaten von Snapshot 10 für die Standardkonfiguration (`root`). Der Bereinigungsalgorithmus ist mit `Zeitleiste` festgelegt.

`snapper --config home modify --description "Tägliche Sicherung" -cleanup-algorithm "Zeitleiste"120`
: Bearbeitet die Metadaten von Snapshot 120 für die benutzerdefinierte Konfiguration `home`. Eine neue Beschreibung wird festgelegt, und der Bereinigungsalgorithmus wird aufgehoben.

4.3.4 Löschen von Snapshots

Zum Löschen eines Snapshots mit dem *Snapper*-Modul in YaST wählen Sie den gewünschten Snapshot in der Liste aus, und klicken Sie auf *Löschen*.

Um einen Snapshot mit dem Kommandozeilenwerkzeug zu löschen, müssen Sie seine Nummer kennen. Führen Sie hierzu `snapper list` aus. Zum Löschen eines Snapshots führen Sie `snapper delete` *`NUMBER`* aus.

TIPP: Löschen von Snapshot-Paaren

Wenn Sie einen `Pre`-Snapshot löschen, müssen Sie auch den zugehörigen `Post`-Snapshot löschen (und umgekehrt).

`snapper delete 65`
: Löscht Snapshot 65 für die Standardkonfiguration (`root`).

`snapper -c home delete 89 90`
: Löscht Snapshots 89 und 90 für die benutzerdefinierte Konfiguration `home`.

TIPP: Alte Snapshots belegen mehr Speicherplatz

Wenn Sie Snapshots löschen, um Speicherplatz auf der Festplatte freizugeben (weitere Informationen finden Sie unter Abschnitt 4.1.1, „Snapshots und Festplattenspeicher“ (S. 32)), löschen Sie zuerst die älteren Snapshots. Je älter ein Snapshot ist, desto mehr Speicherplatz belegt er.

Snapshots werden außerdem im Rahmen eines täglichen CRON-Auftrags automatisch gelöscht. Weitere Informationen finden Sie unter Abschnitt 4.3.1.2, „Bereinigungsalgorithmen“ (S. 46).

4.4 Einschränkungen

Btrfs und Snapper sind für den Einsatz in Produktionsumgebungen bereit, werden jedoch fortlaufend weiterentwickelt. Zurzeit gelten die nachfolgenden Einschränkungen. Diese Punkte sollen in künftigen Versionen behoben werden.

4.4.1 Datenkonsistenz

Es gibt keinen Mechanismus, mit dem die Datenkonsistenz beim Erstellen von Snapshots gewährleistet werden kann. Wenn eine Datei (z. B. eine Datenbank) zur selben Zeit geschrieben wird, während der Snapshot erstellt wird, so wird diese Datei beschädigt oder nur teilweise geschrieben. Beim Wiederherstellen dieser Datei treten Probleme auf. Es wird daher dringend empfohlen, die Liste der geänderten Dateien und ihrer Unterschiede (Diffs) *in jedem Fall* sorgfältig zu prüfen. Stellen Sie nur solche Dateien wieder her, die tatsächlich zu der Aktion gehören, für die das Rollback vorgenommen werden soll.

4.4.2 Rückgängigmachen des Hinzufügens von Benutzern

In der Regel befindet sich das Verzeichnis `/home` auf einer separaten Partition. Eine solche separate Partition gehört nicht zur Standardkonfiguration für YaST-Rollbacks. Aus diesem Grund wird die Home-Partition des Benutzers nicht gelöscht, wenn das Hinzufügen eines Benutzers mit Snapper rückgängig gemacht wird. Für das Entfernen von Benutzern wird dringend das YaST-Werkzeug *Benutzer- und Gruppenverwaltung* empfohlen.

4.4.3 Kein Rollback bei Änderungen an /boot und Bootloadern

Derzeit kann SUSE Linux Enterprise Desktop nicht von einer Btrfs-Partition booten. Bei der Installation wird daher eine separate Partition für `/boot` angelegt, wenn Sie Btrfs für die Systempartition verwenden. Da `/boot` keine Snapshots unterstützt, gelten die folgenden Einschränkungen für YaST-/zypper-Rollbacks:

Kein Rollback von Konfigurationsänderungen am Bootloader
: Die einzige Datei, für die ein Rollback durchgeführt werden kann, ist die Bootloader-Konfigurationsdatei in `/etc`. Die Hauptkonfigurationsdateien befinden sich in `/boot`, und ein Rollback für diese Dateien ist nicht möglich.

Kein vollständiges Rollback für Kernel-Installationen
: Der Kernel selbst und initrd werden in der `/boot`-Partition, intalliert, die Kernel-Module und -Quellen dagegen in `/var/lib` bzw. `/usr/src`. Bei jeder Kernel-Installation werden außerdem die Bootloader-Konfigurationsdateien in /boot geändert. Wenn Sie also ein Rollback vornehmen, bei dem eine Kernel-Installation rückgängig gemacht werden soll, müssen Sie den Kernel und initrd manuell von /boot entfernen und den Boot-Eintrag für den Kernel aus der Bootloader-Konfiguration löschen.

4.5 Häufig gestellte Fragen

Warum zeigt Snapper keine Änderungen in `/var/log`, `/tmp` und anderen Verzeichnissen an?
: Für einige Verzeichnisse wurde das Anfertigen von „Snapshots“ bewusst deaktiviert, beispielsweise für `/var/log`, da das Rückgängigmachen von Protokollen die Suche nach Problemen erschweren würde. Sollen für einen Pfad keine „Snapshots“ angefertigt werden, legen Sie ein Subvolume für diesen Pfad an. Die folgenden Einhängepunkte werden beim Anfertigen von „Snapshots“ unter SUSE Linux Enterprise Desktop nicht berücksichtigt:

  - `/opt`
  - `/srv`
  - `/tmp`
  - `/var/crash`
  - `/var/log`
  - `/var/run`
  - `/var/spool`

- `/var/tmp`

Kann ich einen Snapshot über den Bootloader booten?
: Dies ist zurzeit nicht möglich. Der Bootloader unter SUSE Linux Enterprise Desktop bietet zurzeit keine Unterstützung für das Booten von einer `Btrfs`-Partition.

4.6 Verwenden von Snapper auf Thin Provisioned LVM-Volumes

Neben Snapshots auf `Btrfs`-Dateisystemen unterstützt Snapper auch das Anfertigen von „Snapshots" auf Thin Provisioned LVM-Volumes (Snapshots auf normalen LVM-Volumes werden *nicht* unterstützt), die mit ext3 oder XFS formatiert sind. Weitere Informationen sowie Anweisungen zur Einrichtung finden Sie unter Abschnitt „LVM-Konfiguration" (Kapitel 12, *Fortgeschrittene Festplattenkonfiguration*, ↑*Bereitstellungshandbuch*).

Um Snapper auf einem Thin Provisioned LVM-Volume zu nutzen, müssen Sie eine Snapper-Konfiguration für dieses Volume erstellen. Auf LVM muss das Dateisystem mit `--fstype=lvm(`*`FILESYSTEM`*`)` angegeben werden. Zurzeit werden ext3 und XFS unterstützt; `ext3` und `xfs` sind damit gültige Werte für *`FILESYSTEM`*. Beispiel:

```
snapper -c lvm create-config --fstype="lvm(xfs)" /thin_lvm
```

Sie können diese Konfiguration gemäß den Anweisungen unter Abschnitt 4.2.3.1, „Anpassen der Konfigurationsdatei" (S. 41) an Ihre Anforderungen anpassen. Nun können Sie mit Snapper arbeiten und dabei Snapshots erstellen und verwalten, Dateien wiederherstellen und Änderungen rückgängig machen.

Fernzugriff mit VNC

5

Mit Virtual Network Computing (VNC) können Sie einen Remote-Computer über einen grafischen Desktop steuern (anders als bei einem Remote-Shell-Zugriff). VNC ist plattformunabhängig und ermöglicht Ihnen den Zugriff auf den Remote-Rechner über ein beliebiges Betriebssystem.

SUSE Linux Enterprise Desktop unterstützt zwei verschiedene Arten von VNC-Sitzungen: einmalige Sitzungen, die so lange „aktiv" sind, wie die VNC-Verbindung zum Client besteht, und permanente Sitzungen, die so lange „aktiv" sind, bis sie explizit beendet werden.

ANMERKUNG: Sitzungstypen

Ein Rechner kann beide Sitzungen gleichzeitig auf verschiedenen Ports bieten, eine geöffnete Sitzung kann jedoch nicht von einem Typ in den anderen konvertiert werden.

5.1 Einmalige VNC-Sitzungen

Eine einmalige Sitzung wird vom Remote-Client initiiert. Sie startet einen grafischen Anmeldebildschirm auf dem Server. Auf diese Weise können Sie den Benutzer auswählen, der die Sitzung starten soll sowie, sofern vom Anmeldungsmanager unterstützt, die Desktop-Umgebung. Sobald Sie die Client-Verbindung, beispielsweise eine VNC-Sitzung, beenden, werden auch alle während der Sitzung gestarteten Anwendungen beendet. Einmalige VNC-Sitzungen können nicht freigegeben werden, Sie können jedoch mehrere Sitzungen gleichzeitig auf demselben Host ausführen.

***Prozedur 5.1** Aktivieren von einmaligen VNC-Sitzungen*

1 Starten Sie *YaST* > *Netzwerkdienste* > *Verwaltung von entfernten Rechnern aus (remote) (VNC)*.

2 Aktivieren Sie *Verwaltung via entfernten Rechner (remote) erlauben*.

3 Aktivieren Sie bei Bedarf *Firewall-Port öffnen* (wenn Ihre Netzwerkschnittstelle z. B. so konfiguriert ist, dass sie in der externen Zone liegt). Wenn Sie mehrere Netzwerkschnittstellen haben, beschränken Sie das Öffnen der Firewall-Ports über *Firewall-Details* auf eine bestimmte Schnittstelle.

4 Bestätigen Sie die Einstellungen mit *Beenden*.

5 Falls zu dem Zeitpunkt noch nicht alle erforderlichen Pakete verfügbar sind, müssen Sie der Installation der fehlenden Pakete zustimmen.

ANMERKUNG: Verfügbare Konfigurationen

Die Standardkonfiguration von SUSE Linux Enterprise Desktop stellt Sitzungen mit einer Auflösung von 1024 x 768 Pixeln und einer Farbtiefe von 16 Bit bereit. Die Sitzungen sind an Port `5901` für „reguläre" VNC-Viewer (entspricht VNC-Display `1`) und an Port `5801` für Webbrowser verfügbar.

Weitere Konfigurationen können an anderen Ports verfügbar gemacht werden.Wenden Sie sich an Ihren Systemverwalter.

VNC-Anzeigenummern und X-Anzeigenummern sind bei einmaligen Sitzungen unabhängig. Eine VNC-Anzeigenummer wird manuell jeder Konfiguration zugewiesen, die vom Server unterstützt wird (:1 im obigen Beispiel). Immer, wenn eine VNC-Sitzung mit einer der Konfigurationen initiiert wird, erhält sie automatisch eine freie X-Display-Nummer.

5.1.1 Initiieren einer einmaligen VNC-Sitzung

Um eine einmalige VNC-Sitzung zu initiieren, muss auf dem Client-Rechner ein VNC-Viewer installiert sein. Der Standard-Viewer der SUSE Linux-Produkte ist `vncviewer`,

der sich im Paket `tightvnc` befindet. Sie können eine VNC-Sitzung auch mit Ihrem Webbrowser über ein Java-Applet anzeigen.

Mit folgendem Kommando können Sie den VNC-Viewer starten und eine Sitzung mit der Standardkonfiguration des Servers initiieren:

```
vncviewer jupiter.example.com:1
```

Anstelle der VNC-Anmeldenummer können Sie auch die Portnummer mit zwei Doppelpunkten angeben:

```
vncviewer jupiter.example.com::5901
```

Alternativ können Sie einen Java-fähigen Webbrowser verwenden, um die VNC-Sitzung anzuzeigen. Geben Sie hierzu folgende URL ein:
`http://jupiter.example.com:5801`.

5.1.2 Konfigurieren einmaliger VNC-Sitzungen

Sie können diesen Abschnitt überspringen, wenn Sie die Standardkonfiguration nicht ändern müssen bzw. möchten.

Einmalige VNC-Sitzungen werden über den `xinetd`-Daemon gestartet. Eine Konfigurationsdatei befindet sich unter `/etc/xinetd.d/vnc`. Standardmäßig bietet sie sechs Konfigurationsblöcke: drei für VNC-Viewer (`vnc1` bis `vnc3`) und drei für Java-Applets (`vnchttpd1` bis `vnchttpd3`). Standardmäßig sind nur `vnc1` und `vnchttpd1` aktiv.

Um eine Konfiguration zu aktivieren, können Sie die Zeile `disable = yes` mit dem Zeichen # in der ersten Spalte auskommentieren oder die Zeile vollständig löschen. Wenn Sie eine Konfiguration deaktivieren möchten, dann entfernen Sie das Kommentarzeichen oder fügen Sie diese Zeile hinzu.

Der `Xvnc`-Server kann über die Option `server_args` konfiguriert werden – eine Liste der Optionen finden Sie mit `Xnvc --help`.

Achten Sie beim Hinzufügen benutzerdefinierter Konfigurationen darauf, keine Ports zu verwenden, die bereits von anderen Konfigurationen, anderen Services oder bestehenden permanenten VNC-Sitzungen auf demselben Host verwendet werden.

Aktivieren Sie Konfigurationsänderungen mit folgendem Kommando:

```
rcxinetd reload
```

WICHTIG: Firewall und VNC-Ports

Wenn Sie die entfernte Verwaltung wie in Prozedur 5.1, „Aktivieren von einmaligen VNC-Sitzungen“ (S. 54) beschrieben aktivieren, werden die Ports `5801` und `5901` in der Firewall geöffnet. Wenn die Netzwerkschnittstelle, über die die VNC-Sitzung bereitgestellt wird, durch eine Firewall geschützt wird, müssen Sie die entsprechenden Ports manuell öffnen, wenn Sie zusätzliche Ports für VNC-Sitzungen aktivieren. Eine Anleitung dazu finden Sie in Chapter 15, *Masquerading and Firewalls* (↑*Security Guide*).

5.2 Permanente VNC-Sitzungen

Eine permanente VNC-Sitzung wird auf dem Server initiiert. Die Sitzung und sämtliche in dieser Sitzungsausführung gestarteten Anwendungen werden ungeachtet der Client-Verbindungen so lange ausgeführt, bis die Sitzung beendet wird.

Auf eine permanente Sitzung kann gleichzeitig von mehreren Clients zugegriffen werden. Dies eignet sich ideal für Demozwecke, bei denen ein Client den vollen Zugriff und alle anderen einen reinen Anzeigezugriff haben. Weiter eignet sich dies für Schulungen, bei denen der Schulungsleiter einen Zugriff auf den Desktop des Teilnehmers benötigt. In den meisten Fällen werden Sie Ihre VNC-Sitzung jedoch nicht freigeben wollen.

Im Gegensatz zu einer einmaligen Sitzung, bei der ein Display-Manager gestartet wird, startet eine permanente Sitzung einen einsatzbereiten Desktop, der unter den Benutzernamen ausgeführt wird, unter dem die VNC-Sitzung gestartet wurde.

Der Zugriff auf permanente Sitzungen wird durch zwei mögliche Arten von Passwörtern geschützt:

- ein reguläres Passwort, das den vollen Zugriff ermöglicht, oder
- ein optionales Passwort, das keinen interaktiven Zugriff ermöglicht und nur eine Anzeige liefert.

Eine Sitzung kann mehrere Client-Verbindungen beider Arten gleichzeitig haben.

Prozedur 5.2 *Starten einer permanenten VNC-Sitzung*

1 Öffnen Sie eine Shell uns stellen Sie sicher, dass Sie als der Benutzer angemeldet sind, der Eigentümer der VNC-Sitzung sein soll.

2 Wenn die Netzwerkschnittstelle, über die die VNC-Sitzung bereitgestellt wird, durch eine Firewall geschützt wird, müssen Sie die von Ihrer Sitzung verwendeten Ports manuell in der Firewall öffnen. Wenn Sie mehrere Sitzungen starten, können ie alternativ einen Portbereich öffnen. Details zur Konfiguration der Firewall finden Sie unter Chapter 15, *Masquerading and Firewalls* (↑*Security Guide*).

`vncserver` verwendet die Port `5901` für Display `:1`, `5902` für Display `:2` usw. Bei permanenten Sitzungen haben das VNC-Display und das X-Display normalerweise dieselbe Nummer.

3 Geben Sie folgendes Kommando ein, um eine Sitzung mit einer Auflösung von 1024x769 Pixel und einer Farbtiefe von 16 Bit zu starten:

```
vncserver -geometry 1024x768 -depth 16
```

Das Kommando `vncserver` verwendet, sofern keine Display-Nummer angegeben ist, eine freie Display-Nummer und gibt seine Auswahl aus. Weitere Optionen finden Sie mit `man 1 vncserver`.

Bei der erstmaligen Ausführung von `vncviewer` wird nach einem Passwort für den vollständigen Zugriff auf die Sitzung gefragt. Geben Sie gegebenenfalls auch ein Passwort für den reinen Anzeigezugriff auf die Sitzung ein.

Die hier angegebenen Passwörter werden auch für zukünftige Sitzungen verwendet, die durch denselben Benutzer gestartet werden. Sie können mit dem Kommando `vncpasswd` geändert werden.

WICHTIG: Sicherheitsüberlegungen

Achten Sie darauf, dass Ihre Passwörter sicher und ausreichend lang sind (mindestens acht Zeichen). Teilen Sie diese Passwörter niemandem mit.

VNC-Verbindungen sind unverschlüsselt. Wenn jemand also die Netzwerke zwischen beiden Computern ausspioniert, kann dieser die Passwörter bei der Übertragung zu Beginn der Sitzung lesen.

Beenden Sie, um die Sitzung zu beenden, die Desktopumgebung, die innerhalb der VNC-Sitzung ausgeführt wird über den VNC-Viewer so, wie Sie eine normale lokale X-Sitzung beenden würden.

Wenn Sie eine Sitzung lieber manuell beenden, öffnen Sie eine Shell auf dem VNC-Server und vergewissern Sie sich, dass Sie als der Benutzer angemeldet ist, der der Eigentümer der zu beendenden VNC-Sitzung ist. Führen Sie das folgende Kommando aus, um die Sitzung zu beenden, die auf Display `:1`: `vncserver -kill :1` ausgeführt wird.

5.2.1 Verbindung zu einer permanenten VNC-Sitzung herstellen

Um eine Verbindung zu einer permanenten VNC-Sitzung herzustellen, muss ein VNC-Viewer installiert sein. Der Standard-Viewer der SUSE Linux-Produkte ist `vncviewer`, der sich im Paket `tightvnc` befindet. Sie können eine VNC-Sitzung auch mit Ihrem Webbrowser über ein Java-Applet anzeigen.

Verwenden Sie das folgende Kommando, um den VNC-Viewer zu starten und eine Verbindung zu Display `:1` auf dem VNC-Server herzustellen

```
vncviewer jupiter.example.com:1
```

Anstelle der VNC-Anmeldenummer können Sie auch die Portnummer mit zwei Doppelpunkten angeben:

```
vncviewer jupiter.example.com::5901
```

Alternativ können Sie einen Java-fähigen Webbrowser verwenden, um die VNC-Sitzung anzuzeigen. Geben Sie hierzu folgende URL ein:
`http://jupiter.example.com:5801`.

5.2.2 Konfigurieren von permanenten VNC-Sitzungen

Permanente VNC-Sitzungen können durch Bearbeiten von `$HOME/.vnc/xstartup` konfiguriert werden. Standardmäßig startet dieses Shell-Skript ein `xterm` und den

`twm`-Fenster-Manager. Um stattdessen entweder GNOME oder KDE zu starten, müssen Sie die mit `twm` beginnende Zeile durch eine der folgenden Zeilen ersetzen:

```
/usr/bin/gnome     # GNOME
/usr/bin/startkde  # KDE
```

ANMERKUNG: Eine Konfiguration pro Benutzer

Permanente VNC-Sitzungen werden jeweils nur einmal pro Benutzer konfiguriert. Mehrere von einem Benutzer gestartete Sitzungen verwenden alle dieselben Start- und Passwortdateien.



GNOME-Konfiguration für Administratoren

6

In diesem Kapitel werden die GNOME-Konfigurationsoptionen vorgestellt, die Administratoren verwenden können, um systemweite Einstellungen anzupassen. Dazu gehören beispielsweise Vorgänge wie Anpassen von Menüs, Installieren von Themen, Konfigurieren von Schriften, Ändern bevorzugter Anwendungen und Sperren von Funktionen.

Diese Konfigurationsoptionen werden im GConf-System gespeichert. Greifen Sie auf das GConf-System mit Tools wie der Kommandozeilenschnittstelle `gconftool-2` oder dem GUI-Tool `gconf-editor` zu.

6.1 Das GConf-System

Der GNOME-Desktop verwaltet seine Konfiguration mit GConf. Dabei handelt es sich um eine hierarchisch strukturierte Datenbank oder Registrierung, in der der Benutzer seine eigenen Einstellungen ändern und der Systemadministrator Standardwerte oder obligatorische Werte für alle Benutzer festlegen kann. Sie gelangen zu den GConf-Einstellungen, indem Sie Zugriffspfade wie `/desktop/gnome/background/picture_filename` angeben. Dieses Beispiel ist der Schlüssel, der den Dateinamen des Desktop-Hintergrundbilds enthält.

Verwenden Sie den grafischen `gconf-editor`, wenn Sie alle Optionen bequem durchsehen möchten. Eine kurze Nutzungsbeschreibung von gconf-editor finden Sie in Abschnitt 6.1.1, „Der grafische gconf-editor“ (S. 62). Falls Sie eine skriptfähige Lösung brauchen, siehe Abschnitt 6.1.2, „Die Kommandozeilenschnittstelle gconftool-2“ (S. 63).

WARNUNG: Dialogfelder im GNOME-Kontrollzentrum

Direkter Zugriff auf das Gconf-System kann das System unbrauchbar machen und sollte daher nur mit äußerster Vorsicht erfolgen.

Unerfahrene Benutzer, die nur einige gängige Desktop-Funktionen ändern möchten, sollten die Konfigurationsdialogfelder des GNOME-Kontrollzentrums verwenden. Um das GNOME-Kontrollzentrum zu starten, klicken Sie auf *Computer* > *Kontrollzentrum*. Weitere Informationen finden Sie in Abschnitt „Das Kontrollzentrum“ (Kapitel 3, *Anpassen Ihrer Einstellungen*, ↑*GNOME-Benutzerhandbuch*).

6.1.1 Der grafische gconf-editor

Mithilfe von gconf-editor können Sie GConf-Einstellungen durchsuchen und interaktiv ändern. Um gconf-editor in der Standardansicht *Einstellungsfenster* zu öffnen, klicken Sie auf *Computer* > *Weitere Anwendungen* und anschließend in der Gruppe *System* auf *GNOME-Konfigurationseditor*.

Standardmäßig können Benutzer die Einstellungen für ihren eigenen Desktop ändern, und der Administrator kann die Einstellungen zur Angabe von Standardwerten oder obligatorischen Werten vorbereiten. Gehen Sie folgendermaßen vor, wenn beispielsweise die Funktion *Tipppause* als obligatorische Funktion für alle Benutzer aktiviert werden soll:

1. Starten Sie `gconf-editor` als `root` in der Kommandozeile.

2. Erweitern Sie im Baumbereich auf der linken Seite den Eintrag `/desktop/gnome/typing_break`.

3. Klicken Sie mit der rechten Maustaste auf *Aktiviert* und wählen Sie *Als obligatorisch festlegen*. Danach können Sie diese Funktion verwalten.

4. Öffnen Sie das Fenster *Notwendige Einstellungen*, indem Sie auf *Datei* > *Neues obligatorisches Fenster* klicken.

5. Erweitern Sie im Baumbereich des Fensters *Obligatorische Einstellungen* den Eintrag `/desktop/gnome/typing_break` und klicken Sie auf *Aktiviert*.

6 Schließen Sie das Fenster, um die Einstellung zu speichern, indem Sie auf *Datei* > *Fenster schließen* klicken.

Weitere Informationen über den gconf-editor finden Sie im Konfigurations-Editor-Handbuch unter http://library.gnome.org/users/gconf-editor/stable/.

6.1.2 Die Kommandozeilenschnittstelle gconftool-2

Verwenden Sie `gconftool-2` zum Ändern von Einstellungen über die Kommandozeile oder in Skripts. Nachfolgend einige Beispiele:

Verwenden Sie als `root` den folgenden Befehl, um die Werte aller Schlüssel aufzulisten:

```
gconftool-2 --recursive-list /
```

Wenn Sie nur an einem Teil der Schlüssel interessiert sind, geben Sie einen Zugriffspfad wie z. B. `/desktop/gnome/typing_break` an:

```
gconftool-2 --recursive-list /desktop/gnome/typing_break
```

So listen Sie obligatorische Einstellungen auf:

```
gconftool-2 --recursive-list \
  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory /
```

So legen Sie eine obligatorische Einstellung wie `typing_break` fest:

```
gconftool-2 \
  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \
  --type bool \
  --set /desktop/gnome/typing_break/enabled true
```

So heben Sie eine obligatorische Einstellung auf:

```
gconftool-2 \
  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \
  --unset /desktop/gnome/typing_break/enabled
```

Verwenden Sie für Standardeinstellungen `/etc/gconf/gconf.xml.default`.

Weitere Informationen zu `gconftool-2` finden Sie im Administratorhandbuch zum GNOME-Desktop-System im Abschnitt zum GConf-Kommandozeilen-Tool unter

http://help.gnome.org/admin/system-admin-guide/2.32/gconf-6.html.en und in der gconftool-2-man-Seite (man gconftool-2).

6.2 Anpassen von Hauptmenü, Kontrollleiste und Application Browser

Steuern Sie die Standardelemente in zahlreichen Abschnitten des Hauptmenüs (*Computer*), indem Sie die folgenden Dateien anpassen:

- **/usr/share/gnome-main-menu/applications.xbel:** Liste der standardmäßig bevorzugten Anwendungen.
- **/usr/share/gnome-main-menu/documents.xbel:** Liste der standardmäßig bevorzugten Dokumente.
- **/usr/share/gnome-main-menu/system-items.xbel:** Im Systemabschnitt angezeigte Elemente.

Mit gconf-editor können Sie die Anzahl der angezeigten Elemente anpassen:

- **/desktop/gnome/applications/main-menu/file-area/min_recent_items:** Mindestanzahl der zuletzt verwendeten Elemente.
- **/desktop/gnome/applications/main-menu/file-area/max_total_items:** Höchstanzahl der zuletzt verwendeten Elemente.

Sie können den Application Browser auf zahlreiche Arten anpassen, z. B. sein Verhalten, wenn Benutzer Objekte starten, oder die Anzahl der angezeigten Elemente in der Kategorie *Neue Anwendungen*. Schlagen Sie die Schlüssel /desktop/gnome/applications/main-menu/ab_* mit gconf-editor nach.

Weitere Informationen finden Sie im Abschnitt über die Anpassung von Menüs im Administratorhandbuch zum GNOME-Desktop-System unter https://help.gnome.org/admin/system-admin-guide/2.32/menustructure-0.html.en.

6.3 Automatischer Start von Anwendungen

Verwenden Sie zum automatischen Start von Anwendungen in GNOME eine der folgenden Methoden:

- **So führen Sie Anwendungen für jeden Benutzer aus:** Platzieren Sie `.desktop`-Dateien in `/usr/share/gnome/autostart`.
- **So führen Sie Anwendungen für einen einzelnen Benutzer aus:** Platzieren Sie `.desktop`-Dateien in `~/.config/autostart`.

Um den automatischen Start einer Anwendung zu deaktivieren, fügen Sie `X-Autostart-enabled=false` zur `.desktop`-Datei hinzu.

6.4 Automatisches Einhängen und Verwalten von Mediengeräten

Nautilus (`nautilus`) überwacht Volume-abhängige Ereignisse und reagiert mit einer vom Benutzer angegebenen Richtlinie. Sie können Nautilus verwenden, um Laufwerke im laufenden Betrieb und eingelegte Wechseldatenträger einzuhängen, Programme automatisch auszuführen und Audio-CDs oder Video-DVDs abzuspielen. Nautilus kann auch automatisch Fotos von Digitalkameras importieren.

Systemadministratoren können systemweite Standards festlegen. Weitere Informationen finden Sie in Abschnitt 6.5, „Ändern von bevorzugten Anwendungen“ (S. 65).

6.5 Ändern von bevorzugten Anwendungen

Die bevorzugten Anwendungen von Benutzern ändern Sie, indem Sie `/etc/gnome_defaults.conf` bearbeiten. Weitere Hinweise finden Sie in dieser Datei.

Nachdem Sie die Datei bearbeitet haben, führen Sie `SuSEconfig --module glib2` aus.

Weitere Informationen über MIME-Typen finden Sie unter http://www.freedesktop.org/Standards/shared-mime-info-spec.

6.6 Verwalten von Profilen mit Sabayon

Sabayon ist ein Werkzeug zur Systemverwaltung, mit dessen Hilfe Desktop-Umgebungsprofile erstellt und angewendet werden können. Bei einem Desktop-Profil handelt es sich um eine Reihe von Standardeinstellungen und Beschränkungen, die entweder auf einzelne Benutzer oder auf Benutzergruppen angewendet werden können. In Sabayon können Sie GConf-Standards und obligatorische Schlüssel mithilfe eines grafischen Tools bearbeiten.

Die Profildefinition erfolgt in einer grafischen Sitzung, ähnlich wie eine Sitzung, die ein Benutzer in einem Desktop-Fenster ausführen würde. Sie können Eigenschaften (wie Desktop-Hintergrund, Symbolleisten und verfügbare Miniprogramme) auf die übliche Weise ändern. Sabayon erkennt auch Änderungen an den Standardeinstellungen in den meisten Desktop-Anwendungen.

Dateien oder Dokumente, die im simulierten Home-Verzeichnis oder auf dem Desktop belassen werden, werden in das fertige Profil aufgenommen. Dies betrifft viele anwendungsspezifische Datenbanken, z. B. Tomboy-Notes. Dieser Mechanismus vereinfacht es, einführende Notizen oder Vorlagen so anzubieten, dass neue Benutzer bequem darauf zugreifen können.

Ein Benutzerprofil kann seine Einstellungen von einem übergeordneten Profil erben und damit spezifische Werte überschreiben oder hinzufügen. Dies ermöglicht hierarchische Sets von Einstellungen. Sie können beispielsweise ein Profil „Angestellte“ definieren und daraus Profile „Künstler“ und „Qualitätssicherung“ ableiten.

Neben dem Bereitstellen von Standards kann Sabayon auch Einstellungen sperren. Dies verhindert, dass Benutzer die Einstellung ändern. Beispiel: Sie können angeben, dass der Desktop-Hintergrund nicht geändert werden kann und immer als der Standard erscheint, den Sie festgelegt haben. Dies verhindert die beiläufige Verfälschung von

Einstellungen und kann damit Anrufe beim Helpdesk verhindern und Kiosk-ähnliche Umgebungen ermöglichen. Jedoch bietet das keine absolute Sicherheit, auf die Verlass wäre.

Sabayon bietet auch eine Liste von Einstellungen für Awendungen und generische Elemente von Benutzeroberflächen, die integrierte Sperrenunterstützung samt OpenOffice.org und die GNOME-Kontrollleiste bieten. Beispielsweise kann die Kontrollleiste so eingerichtet werden, dass nur bestimmte Miniprogramme hinzugefügt werden können und eine Änderung ihrer Position oder Größe am Bildschirm verhindert wird. Ebenso können die Elemente im Menü „Speichern" über alle Anwendungen hinweg deaktiviert werden, damit Benutzer Dokumente nicht speichern können.

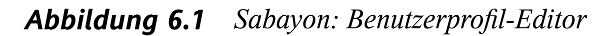
Die Profile sind auf andere Computer übertragbar. Sie befinden sich in `/etc/desktop-profiles/`, und jedes Profil wird in einer separaten ZIP-Datei gespeichert.

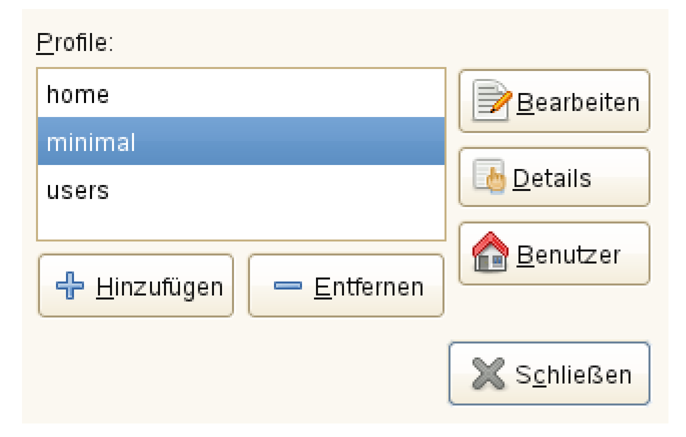
6.6.1 Erstellen eines Profils

Profile werden in ZIP-Dateien unter `/etc/desktop-profiles` gespeichert. Jedes gespeicherte Profil befindet sich in einer separaten ZIP-Datei als *`Name-des-Profils`*`.zip`. Sie können Profile auf andere Computer kopieren oder verschieben.

1. Klicken Sie auf *Computer* > *Weitere Anwendungen* > *System* > *Benutzerprofileditor*.

2. Wenn Sie nicht als `root`-Benutzer angemeldet sind, geben Sie das `root`-Passwort ein und klicken Sie dann auf *Fortfahren*.


***Abbildung 6.1** Sabayon: Benutzerprofil-Editor*



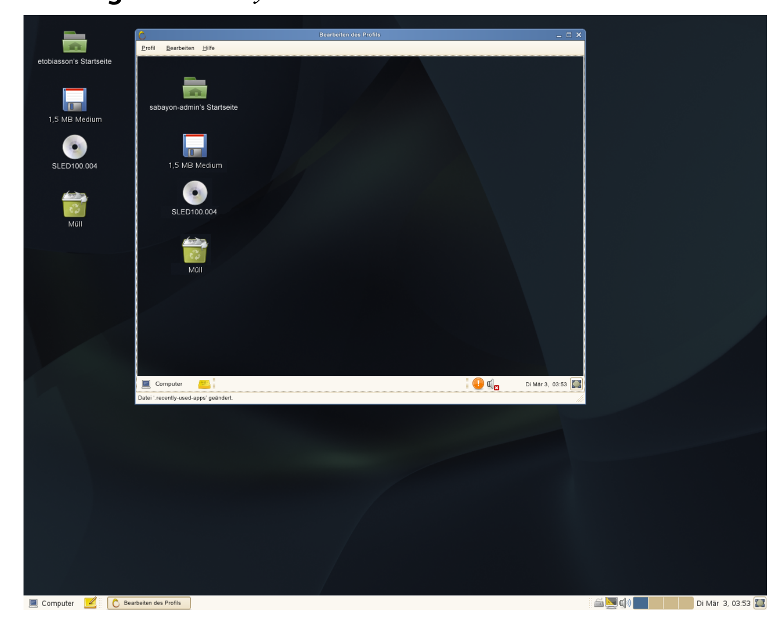
3. Klicken Sie auf *Hinzufügen*.

4. Geben Sie einen Namen für das Profil an und klicken Sie dann auf *Hinzufügen*.

5. Wählen Sie das Profil aus und klicken Sie dann auf *Bearbeiten*.

   Eine neue Desktop-Sitzung wird in einem Xnest-Fenster geöffnet.

Abbildung 6.2 *Sabayon: Neues Xnest-Fenster*



6 Nehmen Sie im Xnest-Fenster die gewünschten Änderungen an den Einstellungen vor.

Jede Einstellung, die Sie ändern, wird im Xnest-Fenster angezeigt.

Sie können eine Einstellung als obligatorisch festlegen (*Bearbeiten* > *Obligatorisches erzwingen*), eine Einstellung ignorieren (*Bearbeiten* > *Ändern* > *Ignorieren*) oder eine Einstellung als Standard festlegen (*Ignorieren* bzw. *Obligatorisch* sind deaktiviert).

7 Um Einstellungen für Benutzer zu sperren, klicken Sie im Xnest-Fenster auf *Bearbeiten* > *Sperren*.

Sie können zwischen den folgenden Optionen auswählen:

Allgemein: Damit ist es möglich, die Funktionen Kommandozeile, Drucken, Druckereinrichtung und Speichern auf Platte zu deaktivieren.

Feld: Damit können Sie die Kontrollleisten sperren sowie erzwungenes Beenden, Bildschirmsperre, Abmeldung und beliebige Miniprogramme in der Liste *Deaktivierte Miniprogramme* deaktivieren.

OpenOffice.org: Ermöglicht Ihnen, die Makro-Sicherheitsstufe für OpenOffice.org-Dokumente, Lade- und Speicheroptionen sowie Optionen für die Benutzeroberfläche zu definieren.

8 Um das Profil zu speichern, klicken Sie auf *Profil* > *Speichern*.

   Das Profil wird unter `/etc/desktop-profiles` gespeichert.

9 Klicken Sie auf *Profil* > *Beenden*, um das Xnest-Fenster zu schließen, und klicken Sie dann auf *Schließen*, um Sabayon zu beenden.

6.6.2 Anwenden eines Profils

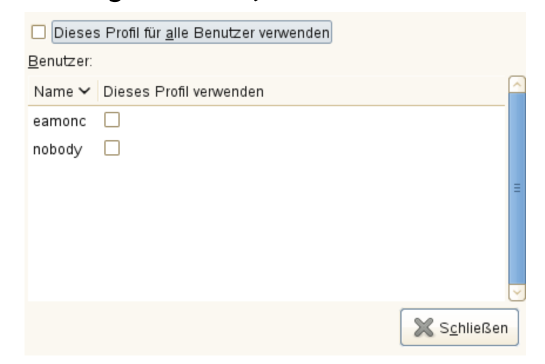
Sie können ein Profil auf einzelne Benutzer oder alle Benutzer einer Arbeitssstation anwenden.

1 Klicken Sie auf *Computer* > *Weitere Anwendungen* > *System* > *Benutzerprofileditor*.

2 Wenn Sie nicht als `root`-Benutzer angemeldet sind, geben Sie das `root`-Passwort ein und klicken Sie dann auf *Fortfahren*.

3 Wählen Sie das gewünschte Profil aus und klicken Sie dann auf *Benutzer*.

Abbildung 6.3 *Sabayon: Auswählen von Benutzern*



4 Wählen Sie die Benutzer aus, die dieses Profil verwenden sollen.

Um dieses Profil auf alle Benutzer an dieser Arbeitsstation anzuwenden, klicken Sie auf *Dieses Profil für alle Benutzer verwenden*.

5 Klicken Sie auf *Schließen*.

6.7 Hinzufügen von Dokumentvorlagen

Füllen Sie zum Hinzufügen von Dokumentvorlagen das Verzeichnis `Templates` im Home-Verzeichnis eines Benutzers. Dies können Sie manuell für jeden Benutzer erledigen, indem Sie die Dateien in `~/Templates` kopieren, oder systemweit, indem Sie das Verzeichnis `Templates` unter `/etc/skel` hinzufügen, bevor der Benutzer erstellt wird.

Ein Benutzer erstellt ein neues Dokument aus einer Vorlage, indem er mit der rechten Maustaste auf den Desktop klickt und *Dokument erstellen* wählt.

6.8 Desktop-Sperrfunktionen

Gelegentlich müssen Desktop-Funktionen oder der Benutzerzugriff auf das zugrunde liegende Betriebssystem entfernt oder deaktiviert werden. GNOME bietet so genannte Sperrfunktionen, um den Desktop entsprechend zu ändern. Genau genommen legen Sie GConf-Schlüssel fest, um diese Änderungen zu implementieren.

Wenn Sie beispielsweise gconf-editor öffnen, sehen Sie Sperrschlüssel für das Hauptmenü in `/desktop/gnome/applications/main-menu/lock-down/application_browser_link_visible`. Dort finden Sie auch Beschreibungen für alle Schlüssel. Die übrigen Sperrschlüssel sind:

/desktop/gnome/lockdown/disable_command_line
: Wenn dies festgelegt ist, werden Terminals nicht im Hauptmenü und im AppBrowser angezeigt.

/apps/panel/global/disable_log_out

/apps/panel/global/disable_lock_screen
Wenn dies festgelegt ist, werden diese Elemente nicht im Hauptmenü angezeigt.

Firefox-Sperrschlüssel finden Sie in `/apps/firefox/lockdown`.

Weitere Informationen finden Sie im „Desktop Administrators' Guide to GNOME Lockdown and Preconfiguration“ von Sayamindu Dasgupta: http://library.gnome.org/admin/deployment-guide/.

6.9 Weiterführende Informationen

Weitere Informationen finden Sie in http://library.gnome.org/admin/.

Verwalten von Software mit Kommandozeilen-Tools 7

Dieses Kapitel behandelt zypper und RPM, zwei Kommandozeilen-Tools zum Verwalten von Software. Eine Definition der in diesem Kontext verwendeten Terminologie (beispielsweise `Repository`, `Patch` oder `Update`) finden Sie unter Abschnitt „Definition der Begriffe“ (Kapitel 6, *Installieren bzw. Entfernen von Software*, ↑*Bereitstellungshandbuch*).

7.1 Verwenden von zypper

Zypper ist ein Kommandozeilen-Paketmanager für Installation, Aktualisierung und Löschung von Paketen sowie zum Verwalten von Repositorys. Die Syntax von Zypper entspricht der von rug. Im Unterschied zu rug benötigt Zypper zur Ausführung im Hintergrund allerdings keinen zmd-Dämon. Weitere Informationen über rug-Kompatibilität finden Sie in `man zypper`, Abschnitt „COMPATIBILITY WITH RUG“. Damit können Sie Software per Fernzugriff oder mithilfe von Shell-Skripten verwalten.

7.1.1 Allgemeine Verwendung

Die allgemeine Syntax von Zypper sieht wie folgt aus:

```
zypper [global-options]command[command-options][arguments] ...
```

Die Komponenten in Klammern sind nicht erforderlich. Am einfachsten führen Sie Zypper aus, indem Sie seinen Namen gefolgt von einem Kommando eingeben. Geben Sie z. B. für das Anwenden aller erforderlichen Patches auf den Systemtyp das Folgende ein:

```
zypper patch
```

Zusätzlich können Sie aus einer oder mehreren globalen Optionen wählen, indem Sie sie direkt vor dem Kommando eingeben. Beispielspielsweise führt `--non-interactive` das Kommando ohne Eingabeaufforderungen aus (und wendet automatisch die Standardantworten an):

```
zypper --non-interactive patch
```

Um die spezifischen Optionen für ein bestimmtes Kommando zu benutzen, geben Sie sie direkt nach dem Kommando ein. Beispielsweise werden mit `--auto-agree-with-licenses` alle erforderlichen Patches auf das System angewendet, ohne eine Bestätigung von Lizenzen anzufordern (sie werden automatisch akzeptiert):

```
zypper patch --auto-agree-with-licenses
```

Einige Kommandos erfordern ein oder mehrere Argumente. Bei der Verwendung des Installationskommandos z. B. müssen Sie angeben, welche Pakete zu installieren sind:

```
zypper install mplayer
```

Einige Optionen erfordern auch ein Argument. Das folgende Kommando listet alle bekannten Muster auf:

```
zypper search -t pattern
```

Sie können alle obigen Optionen kombinieren. Beispielsweise werden mit dem folgenden Kommando `mplayer`- und `amarok`-Pakete mithilfe des `factory`-Repositorys installiert und ausführlich angegeben:

```
zypper -v install --from factory mplayer amarok
```

Mit der Option `--from` bleiben alle Repositorys aktiviert (damit alle Abhängigkeiten aufgelöst werden können), wenn das Paket aus dem angegebenen Repository abrufen wird.

Die meisten Zypper-Kommandos besitzen eine `dry-run`-Option, die eine Simulation des angegebenen Kommandos ausführt. Sie kann für Tests verwendet werden.

```
zypper remove --dry-run MozillaFirefox
```

Zypper unterstützt die globale Option `--userdata` *`string`* zur Identifizierung von Transaktionen. Die benutzerdefinierte Zeichenkette wird an die zypper-Verlaufsprotokolle in `/var/log/zypp/history` und Snapper übergeben.

```
zypper --userdata string patch
```

7.1.2 Installieren und Entfernen von Software mit zypper

Verwenden Sie zur Installation oder Löschung von Paketen die folgenden Kommandos:

```
zypper install package_name
zypper remove package_name
```

Zypper kennt verschiedene Möglichkeiten, Pakete für die Installations- und Löschkommandos anzugeben:

nach dem genauen Namen (und der Versionsnummer) des Pakets

```
zypper install MozillaFirefox
```

oder

```
zypper install MozillaFirefox-3.5.3
```

nach dem Repository-Alias und Paketnamen

```
zypper install mozilla:MozillaFirefox
```

Dabei ist `mozilla` der Alias des Repositorys, aus dem installiert werden soll.

nach dem Paketnamen mit Wildcards
: Das folgende Kommando installiert alle Pakete, deren Name mit „Moz“ beginnt. Verwenden Sie diese Möglichkeit mit äußerster Umsicht, vor allem beim Entfernen von Paketen.

```
zypper install 'Moz*'
```

nach Funktion
: Wenn Sie beispielsweise ein perl-Modul installieren möchten, ohne den Namen des Pakets zu kennen, sind Funktionen praktisch:

```
zypper install 'perl(Time::ParseDate)'
```

nach Funktion und/oder Architektur und/oder Version
: Zusammen mit einer Funktion können Sie eine Architektur (wie `i586` oder `x86_64`) und/oder eine Version angeben. Der Version muss ein Operator voran-

gehen: < (kleiner als), <= (kleiner oder gleich), = (gleich), >= (größer oder gleich), > (größer als).

```
zypper install 'firefox.x86_64'
zypper install 'firefox>=3.5.3'
zypper install 'firefox.x86_64>=3.5.3'
```

nach dem Pfad der RPM-Datei
: Sie können einen lokalen oder entfernten Pfad zu einem Paket angeben:

```
zypper install /tmp/install/MozillaFirefox.rpm
zypper install
http://download.opensuse.org/repositories/mozilla/SUSE_Factory/x86_64/MozillaFirefox-3.5.3-1.3.x86_64.rpm
```

Zum gleichzeitigen Installieren und Entfernen von Paketen verwenden Sie die Modifikatoren `+/-`. Zum gleichzeitigen Installieren von `emacs` und Entfernen von `vim` verwenden Sie Folgendes:

```
zypper install emacs -vim
```

Zum gleichzeitigen Entfernen von `emacs` und Installieren von `vim` verwenden Sie Folgendes:

```
zypper remove emacs +vim
```

Um zu vermeiden, dass der mit - beginnende Paketname als Kommandooption interpretiert wird, verwenden Sie ihn stets als das zweite Argument. Falls dies nicht möglich ist, stellen Sie ihm `--` voran:

```
zypper install -emacs +vim       # Wrong
zypper install vim -emacs        # Correct
zypper install -- -emacs +vim    # same as above
zypper remove emacs +vim         # same as above
```

Wenn Sie (zusammen mit einem bestimmten Paket) alle Pakete entfernen möchten, die nach dem Entfernen dieses Pakets nicht mehr erforderlich sind, verwenden Sie die Option `--clean-deps`:

```
rm package_name --clean-deps
```

Standardmäßig verlangt Zypper eine Bestätigung, bevor ein ausgewähltes Paket installiert oder entfernt wird oder wenn ein Problem auftritt. Mit der Option `--non-interactive` können Sie dieses Verhalten deaktivieren. Die Option muss jedoch vor dem tatsächlich auszuführenden Kommando (`Installieren`, `Entfernen` oder `Patch`) angegeben werden, wie im Folgenden:

```
zypper --non-interactive install package_name
```

Mit dieser Option kann Zypper auch in Skripten und Cron-Aufträgen verwendet werden.

WARNUNG: Entfernen Sie keine obligatorischen Systempakete.

Entfernen Sie keine Pakete wie `glibc`, `zypper`, `kernel` oder ähnliche Pakete. Diese Pakete sind obligatorisch für das System. Wenn sie entfernt werden, kann das System instabil werden oder seine Funktion komplett einstellen.

7.1.2.1 Installieren und Herunterladen von Quellpaketen

Wenn Sie das entsprechende Quellpaket eines Pakets installieren möchten, verwenden Sie:

```
zypper source-install package_name
```

Dieses Kommando installiert auch die Build-Abhängigkeiten des angegebenen Pakets. Wenn Sie dies nicht wünschen, fügen Sie den Schalter `-D` hinzu. Um nur die Build-Abhängigkeiten zu installieren, verwenden Sie `-d`.

```
zypper source-install -D package_name # source package only
zypper source-install -d package_name # build dependencies only
```

Natürlich gelingt dies nur, wenn das Repository mit den Quellpaketen in Ihrer Repository-Liste aktiviert ist (es wird standardmäßig hinzugefügt, aber nicht aktiviert). Details zur Repository-Verwaltung finden Sie unter Abschnitt 7.1.5, „Verwalten von Repositorys mit zypper“ (S. 85).

Eine Liste aller Quellpakete, die in Ihren Repositorys verfügbar sind, können Sie wie folgt abrufen:

```
zypper search -t srcpackage
```

Wenn Sie möchten, können Sie die Quellpakete für alle installierten Pakete in ein lokales Verzeichnis herunterladen. Zum Herunterladen von Quellpaketen verwenden Sie:

```
zypper source-download
```

Das Standardverzeichnis für heruntergeladene Dateien lautet `/var/cache/zypper/source-download`. Mit der Option `--directory` können Sie dieses Verzeichnis ändern. Sollen nur fehlende oder überzählige Pakete angezeigt werden, ohne Pakete

herunterzuladen oder zu löschen, verwenden Sie die Option `--status`. Zum Löschen überzähliger Pakete verwenden Sie die Option `--delete`. Soll das Löschen deaktiviert werden, verwenden Sie die Option `--no-delete`.

7.1.2.2 Dienstprogramme

Wenn Sie prüfen möchten, ob alle Abhängigkeiten noch erfüllt sind, und fehlende Abhängigkeiten reparieren möchten, verwenden Sie:

```
zypper verify
```

Zusätzlich zu Abhängigkeiten, die erfüllt sein müssen, „empfehlen" einige Pakete andere Pakete. Diese empfohlenen Pakete werden installiert, wenn sie aktuell verfügbar und installierbar sind. Falls empfohlene Pakete erst nach der Installation des empfehlenden Pakets (durch Hinzufügen zusätzlicher Pakete oder zusätzlicher Hardware) zur Verfügung steht, verwenden Sie das folgende Kommando:

```
zypper install-new-recommends
```

Dieses Kommando ist nach dem Anschließen einer Webcam oder eines WLAN-Geräts äußerst nützlich. Hiermit werden Treiber für das Gerät und die zugehörige Software installiert, sofern verfügbar. Die Treiber und die zugehörige Software sind nur dann installierbar, wenn bestimmte Hardware-Abhängigkeiten erfüllt sind.

7.1.3 Aktualisieren von Software mit zypper

Es gibt drei verschiedene Möglichkeiten, Software mithilfe von Zypper zu installieren: durch Installation von Patches, durch Installation einer neuen Version eines Pakets oder durch Aktualisieren der kompletten Distribution. Letzters wird mit dem Kommando `zypper dist-upgrade` erreicht, das in Abschnitt 7.1.4, „Distributions-Upgrade mit Zypper" (S. 82) behandelt wird.

7.1.3.1 Installieren von Patches

Um alle offiziell herausgegebenen Patches für Ihr System zu installieren, führen Sie einfach Folgendes aus:

```
zypper patch
```

In diesem Fall werden alle in Ihren Repositorys vorhandenen Patches auf Relevanz überprüft und bei Bedarf installiert. Nach dem Registrieren Ihrer SUSE Linux Enterprise Desktop-Installation wird Ihrem System ein offizielles Aktualisierungs-Repository hinzugefügt, das solche Patches enthält. Das obige Kommando ist alles, was Sie brauchen, um sie bei Bedarf anzuwenden.

Zypper kennt drei unterschiedliche Kommandos, um die Verfügbarkeit von Patches abzufragen:

`zypper patch-check`
: Listet die Anzahl der benötigten Patches auf (Patches, die für Ihr System gelten, aber noch nicht installiert sind)

```
~ # zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

`zypper list-patches`
: Listet alle benötigten Patches auf (Patches, die für Ihr System gelten, aber noch nicht installiert sind)

```
~ # zypper list-patches
Loading repository data...
Reading installed packages...

Repository                          | Name      | Version | Category | Status
------------------------------------+-----------+---------+----------+-------
Updates for openSUSE 11.3 11.3-1.82 | lxsession | 2776    | security | needed
```

`zypper patches`
: Listet alle für SUSE Linux Enterprise Desktop verfügbaren Patches auf, unabhängig davon, ob sie bereits installiert sind oder für Ihre Installation gelten.

Sie können auch Patches für bestimmte Probleme auflisten und installieren. Dazu geben Sie das Kommando `zypper list-patches` mit den folgenden Optionen ein:

`--bugzilla[=`*`Nummer`*`]`
: Listet alle erforderlichen Patches für Probleme mit Bugzilla auf. Optional können Sie eine Fehlernummer angeben, wenn nur Patches für diesen bestimmten Fehler aufgeführt werden sollen.

`--cve[=number]`
: Listet alle erforderlichen Patches für CVE-Probleme (Common Vulnerabilities and Exposures, häufige Sicherheitslücken und Gefährdungen) auf bzw. nur Patches für eine bestimmte CVE-Nummer, sofern angegeben. Standardmäßig werden nur Patches aufgeführt, die noch nicht angewendet wurden. Mit `-a` werden alle Einträge angezeigt.

Zum Installieren eines Patches für ein bestimmtes Bugzilla- oder CVE-Problem verwenden Sie die folgenden Kommandos:

```
zypper patch --bugzilla=number
```

oder

```
zypper patch --cve=number
```

Zum Installieren eines Sicherheits-Patches mit der CVE-Nummer `CVE-2010-2713` führen Sie beispielsweise Folgendes aus:

```
zypper patch --cve=CVE-2010-2713
```

7.1.3.2 Installieren von Updates

Wenn ein Repository neue Pakete enthält, aber keine Patches zur Verfügung stellt, zeigt `zypper patch` keinerlei Wirkung. Verwenden Sie zum Aktualisieren aller installierten Pakete mit neueren verfügbaren Versionen:

```
zypper update
```

Zum Aktualisieren einzelner Pakete geben Sie das Paket mit dem Aktualisierungs- oder Aktualisierungskommando an:

```
zypper update package_name
zypper install package_name
```

Mit dem Kommando kann eine Liste mit allen neuen installierbaren Paketen abgerufen werden.

```
zypper list-updates
```

Dieses Kommando listet ausschließlich Pakete auf, die die folgenden Kriterien erfüllen:

- stammt von demselben Hersteller wie das bereits installierte Paket,

- umfasst Repositorys mit mindestens derselben Priorität wie das bereits installierte Paket,

- ist installierbar (alle Abhängigkeiten wurden erfüllt).

Eine Liste *aller* neuen verfügbaren Pakete (unabhängig davon, ob diese Pakete installierbar sind oder nicht) erhalten Sie mit Folgendem:

```
zypper list-updates --all
```

Um festzustellen, warum ein neues Paket nicht installiert werden kann, verwenden Sie einfach das Kommando `zypper install` oder `zypper update`, wie oben beschrieben.

7.1.3.3 Aktualisieren auf eine neue Produktversion

Um die Installation schnell und einfach auf eine neue Produktversion zu aktualisieren (beispielsweise von SUSE Linux Enterprise Server 11 auf SUSE Linux Enterprise Server 11 SP1), passen Sie zunächst die Repositorys so an, dass sie den aktuellen Repositorys für SUSE Linux Enterprise Desktop entsprechen. Detaillierte Informationen finden Sie in Abschnitt 7.1.5, „Verwalten von Repositorys mit zypper“ (S. 85). Führen Sie dann das Kommando `zypper dist-upgrade` für die erforderlichen Repositorys aus. Dieses Kommando stellt sicher, dass alle Pakete aus den aktuell aktivierten Repositorys installiert werden. Siehe dazu Abschnitt 7.1.4, „Distributions-Upgrade mit Zypper“ (S. 82).

Um das Distributions-Upgrade auf Pakete aus einem bestimmten Repository zu beschränken, während gleichzeitig die anderen Repositorys im Hinblick auf die Abhängigkeiten berücksichtigt werden, verwenden Sie die Option `--from` option und geben Sie das Repository wahlweise mit dem Alias, der Nummer oder der URI an.

ANMERKUNG: Unterschiede zwischen `zypper update` und `zypper dist-upgrade`

Wählen Sie `zypper update`, um Pakete auf neuere Versionen zu aktualisieren, die für Ihre Produktversion verfügbar sind, und die Systemintegrität beizubehalten. `zypper update` richtet sich nach den folgenden Regeln:

keine Herstelleränderungen
keine Architekturänderungen

keine Zurückstufung
installierte Pakete behalten

Bei `zypper dist-upgrade` werden alle Pakete aus den derzeit aktivierten Repositorys installiert. Diese Regel ist erzwungen, d. h. Pakete könnten einen anderen Hersteller oder eine andere Architektur haben oder sogar zurückgestuft werden. Alle Pakete, die nach der Aktualisierung unerfüllte Abhängigkeiten aufweisen, werden deinstalliert.

7.1.4 Distributions-Upgrade mit Zypper

Mit dem Kommandozeilenprogramm `zypper` können Sie ein Upgrade zur nächsten Version der Distribution durchführen. Dabei ist am wichtigsten, dass Sie das System-Upgrade aus dem laufenden System heraus initiieren können.

Diese Funktion ist nützlich für fortgeschrittene Benutzer, die Remote-Upgrades oder Upgrades auf vielen ähnlich konfigurierten Systemen ausführen möchten.

7.1.4.1 Vor dem Start des Upgrades mit Zypper

Zur Vermeidung von unerwarteten Fehlern beim Upgrade-Vorgang mit `zypper` minimieren Sie riskante Konstellationen.

- Schließen Sie möglichst viele Anwendungen und nicht benötigte Services und melden Sie alle regulären Benutzer ab.

- Deaktivieren Sie Repositorys von anderen Herstellern, bevor Sie mit dem Upgrade beginnen, oder verringern Sie die Priorität dieser Repositorys, um sicherzustellen, dass Pakete der Standard-System-Repositorys Vorrang erhalten. Aktivieren Sie sie nach dem Upgrade erneut und bearbeiten Sie ihre Versionsangabe mit der Versionsnummer der Distribution des aufgerüsteten laufenden Systems.

- Das System muss registriert sein. Falls dies noch nicht der Fall ist, registrieren Sie es wahlweise mit dem *Novell Customer Center Configuration*-Modul in YaST oder mit dem Kommandozeilenwerkzeug `suse_register`. Damit werden die Quellen für das System aktualisiert.

WARNUNG: Ausführen von Aufrüstungen ab Neustart

Die Aufrüstung muss komplett von Beginn an bis zum Neustart ausgeführt werden. Es gibt nur eine sehr geringe Chance, Änderungen wieder rückgängig zu machen. Außerdem muss der Server während des gesamten Vorgangs online bleiben.

7.1.4.2 Der Upgrade-Vorgang

WARNUNG: Prüfen der Systemsicherung

Prüfen Sie vor dem Upgrade, ob Ihre Systemsicherung auf dem neuesten Stand und wiederherstellbar ist. Dies ist besonders wichtig, da viele der folgenden Schritte manuell durchgeführt werden müssen.

Das Programm `zypper` unterstützt lange und kurze Kommandonamen. So können Sie `zypper install` z. B. als `zypper in` abkürzen. Im folgenden Text werden die kurzen Varianten verwendet.

Melden Sie sich als `root` an und führen Sie die folgenden Schritte aus:

1 Aktualisieren Sie alle Dienste und Repositorys:

```
zypper ref -s
```

2 Installieren Sie ggf. die Aktualisierungen für die Paketverwaltung:

```
zypper up -t patch
```

Weitere Informationen finden Sie unter Kapitel 1, *YaST-Online-Aktualisierung* (S. 3).

3 Wiederholen Sie Schritt 2 (S. 83) und installieren Sie alle verfügbaren Aktualisierungen für das System.

Hinweis: Soll das obige Kommando in einem Skript für die unbeaufsichtigte Aufrüstung eingesetzt werden, verwenden Sie das folgende Kommando:

```
zypper --non-interactive patch --auto-agree-with-licenses --with-interactive
```

4 Lesen Sie die Informationen zu den Migrationsprodukten in `/etc/products.d/*.prod`. Die installierten Produkte enthalten Informationen zu den Distributionsaufrüstungen sowie zu den Migrationsprodukten, die für die Migration installiert werden sollten. Installieren Sie diese Produkte mit den folgenden Kommandos:

4a Extrahieren Sie die Produktinformationen:

```
zypper se -t product | grep -h -- "-migration" | cut -d\| -f2
```

Ein Beispiel für die Ausgabe:

```
SUSE_SLES-SP3-migration
sle-sdk-SP3-migration
```

4b Installieren Sie diese Migrationsprodukte (Beispiel):

```
zypper in -t product sle-sdk-SP3-migration SUSE_SLES-SP3-migration
```

4c Registrieren Sie die Produkte, damit die entsprechenden Aktualisierungs-Repositorys verfügbar werden:

```
suse_register -d 2 -L /root/.suse_register.log
```

WARNUNG: Aktivieren eines zusätzlichen Repositorys für SLED-Benutzer

Einige devel-Pakete wurden vom `SLED11-SP2`-Installationsmedium in das Repository `SLED11-Extras` verschoben. Damit beim Aufrüsten keine Abhängigkeitskonflikte auftreten, aktualisieren Sie dieses Repository, bevor Sie die eigentliche Aufrüstung starten. Führen Sie `yast2 repositories` aus und aktivieren Sie dort den Eintrag `SLED11-Extras`. Unter SLES ist dieser zusätzliche Schritt nicht erforderlich.

---

5 Aktualisieren Sie die Dienste und Repositorys:

```
zypper ref -s
```

6 Prüfen Sie die Repositorys mit `zypper lr`. Deaktivieren Sie bei Bedarf die SP1/SP2-Repositorys in `Pool/Core/Updates` manuell und aktivieren Sie die neuen SP3-Repositorys (`SP3-Pool`, `SP3-Updates`):

```
zypper mr --disable REPOALIAS
zypper mr --enable REPOALIAS
```

7 Führen Sie eine Distributionsaufrüstung mit dem folgenden Kommando aus (Beispiel für SLES; bei SLED sind die Katalognamen entsprechend zu ändern):

```
zypper dup --from SLES11-SP3-Pool --from SLES11-SP3-Updates
```

Hier können Sie weitere Kataloge hinzufügen, beispielsweise wenn Add-on-Produkte installiert sind. zypper meldet, dass das Migrationsprodukt gelöscht wird und die Hauptprodukte aktualisiert werden. Bestätigen Sie die Meldung. Damit wird die Aktualisierung der rpm-Pakete fortgesetzt.

8 Registrieren Sie die neuen Produkte nach Abschluss der Aufrüstung erneut:

```
suse_register -d 2 -L /root/.suse_register.log
```

9 Booten Sie das System neu:

```
shutdown -r
```

7.1.5 Verwalten von Repositorys mit zypper

Sämtliche Installations- und Patch-Kommandos von Zypper sind von der Liste der bekannten Repositorys abhängig. Um alle dem System bekannten Repositorys aufzulisten, verwenden Sie das Kommando:

```
zypper repos
```

Das Ergebnis ist der folgenden Ausgabe ähnlich:

Beispiel 7.1 *Zypper – Liste der bekannten Repositorys*

```
# | Alias                              | Name
   | Enabled | Refresh
--+-----------------------------------+-----------------------------------+---------+--------
1 | SUSE-Linux-Enterprise-Server 11-0 | SUSE-Linux-Enterprise-Server 11-0
 | Yes     | No
2 | SLES-11-Updates                    | SLES 11 Online Updates
   | Yes     | Yes
```

```
3 | broadcomdrv                       | Broadcom Drivers
   | Yes      | No
```

Bei der Angabe von Repositorys kann in verschiedenen Kommandos ein Alias, URI oder eine Repository-Nummber aus der Ausgabe des Kommandos `zypper repos` verwendet werden. Ein Repository-Alias ist eine Kurzform des Repository-Namens, der in Repository-Kommandos verwendet wird. Beachten Sie dabei, dass sich die Repository-Nummern nach dem Bearbeiten der Repository-Liste ändern können. Der Alias ändert sich nie von alleine.

Standardmäßig werden Details wie URI oder Priorität des Repositorys nicht angezeigt. Verwenden Sie das folgende Kommando, um alle Details aufzulisten:

```
zypper repos -d
```

Unter Umständen enthält die Liste eine Vielzahl an nicht aktivierten Repositorys, was verwirrend wirken kann. Mit dem folgenden Kommando werden ausschließlich aktivierte Repositorys angezeigt:

```
zypper repos -E
```

7.1.5.1 Hinzufügen von Repositorys

WARNUNG: Mögliche Systemkonflikte beim Hinzufügen von Repositorys mit zypper

Standardmäßig werden die Integrität und der Ursprung der Digests und Signaturen überprüft, die aus Paketen in Repositorys von SUSE stammen. Diese „GPG-Prüfung“ wird in der Repository-Konfigurationsdatei auf dem Server aktiviert, der das betreffende Repository bereitstellt.

Beim Hinzufügen eines Repository mit dem Kommando `zypper ar` wird diese Konfigurationsdatei in `/etc/zypp/repos.d` heruntergeladen. zypper informiert den Benutzer außerdem über die Option zur GPG-Prüfung:

```
GPG check: Yes
```

Die Ausgabe der GPG-Prüfung muss stets auf „Ja“ eingestellt sein. Bei „Nein“ können mögliche Konflikte im System auftreten, beispielsweise durch Paket-Downgrades, mit denen bereits behobene Schwachstellen wieder eingebracht werden. Es wird empfohlen, alle Repositorys, bei denen diese Option auf „Nein“ eingestellt ist, als nicht vertrauenswürdig zu betrachten. Falls Sie sicher sind,

dass die GPG-Prüfung versehentlich deaktiviert wurde, aktivieren Sie die Option wieder. Fügen Sie hierzu die folgende Zeile in die entsprechende Repository-Konfigurationsdatei in `/etc/zypp/repos.d` ein:

```
gpgcheck=1
```

Zum Hinzufügen eines Repositorys führen Sie Folgendes aus:

```
zypper addrepo URIalias
```

URI kann ein Internet-Repository, eine Netzwerkressource, ein Verzeichnis oder eine CD oder DVD sein (für Details siehe http://en.opensuse.org/openSUSE:Libzypp_URIs). Der *Alias* ist ein Kürzel und eine eindeutige Kennung für das Repository. Sie können ihn frei wählen, vorausgesetzt, er ist eindeutig. Zypper gibt eine Warnung aus, wenn Sie einen Alias angeben, der bereits verwendet wird.

7.1.5.2 Entfernen von Repositorys

Wenn ein Repository von der Liste entfernt werden soll, verwenden Sie das Kommando `zypper removerepo` zusammen mit dem Alias oder der Nummer des zu löschenden Repositorys. Zum Entfernen des Repositorys, das im dritten Eintrag in Beispiel 7.1, „Zypper – Liste der bekannten Repositorys“ (S. 85) aufgeführt ist, verwenden Sie beispielsweise das folgende Kommando:

```
zypper removerepo 3
```

7.1.5.3 Ändern von Repositorys

Aktivieren oder deaktivieren von Repositorys mit `zypper modifyrepo`. Mit diesem Kommando können Sie auch die Eigenschaften des Repositorys (z. B. Aktualisierungsverhalten, Name oder Priorität) ändern. Das folgende Kommando aktiviert das Repository mit dem Namen `updates`, aktiviert die automatische Aktualisierung und stellt seine Priorität auf 20 ein:

```
zypper modifyrepo -er -p 20 'updates'
```

Das Ändern von Repositorys ist nicht auf ein einziges Repository beschränkt – Sie können auch Gruppen bearbeiten:

`-a`: alle Repositorys

`-l`: lokale Repositorys

`-t`: entfernte Repositorys
`-m TYPE`: Repositorys eines bestimmten Typs (wobei *TYPE* eines der folgenden sein kann: `http`, `https`, `ftp`, `cd`, `dvd`, `dir`, `file`, `cifs`, `smb`, `nfs`, `hd`, `iso`)

Zum Umbenennen eines Repository-Alias verwenden Sie das Kommando `renamerepo`. Das folgende Beispiel ändert den Alias von `Mozilla Firefox` in `firefox`:

```
zypper renamerepo 'Mozilla Firefox' firefox
```

7.1.6 Abfragen von Repositorys und Paketen mit Zypper

Zypper bietet zahlreiche Methoden zur Abfrage von Repositorys oder Paketen. Verwenden Sie die folgenden Kommandos, um eine Liste aller verfügbaren Produkte, Muster, Pakete oder Patches zu erhalten:

```
zypper products
zypper patterns
zypper packages
zypper patches
```

Zur Abfrage aller Repositorys auf bestimmte Pakete verwenden Sie `search`. Es gilt für Paketnamen oder optional für Paketzusammenfassungen und -beschreibungen. Verwenden der Platzhalter `*` und `?`mit dem Suchbegriff ist erlaubt. Standardmäßig unterscheidet der Suchvorgang keine Groß- und Kleinschreibung.

```
zypper search firefox       # simple search for "firefox"
zypper search "*fire*"      # using wild cards
zypper search -d fire      # also search in package descriptions and summaries
zypper search -u firefox    # only display packages not already installed
```

Verwenden Sie zur Suche nach Paketen, die eine spezielle Funktion bieten, das Kommando `what-provides`. Wenn Sie beispielsweise wissen möchten, welches Paket das perl-Modul `SVN::Core` bereitstellt, verwenden Sie das folgende Kommando:

```
zypper what-provides 'perl(SVN::Core)'
```

Um einzelne Pakete abzufragen, verwenden Sie `info` mit einem exakten Paketnamen als Argument. Damit werden detaillierte Informationen zu einem Paket angezeigt. Um auch die Elemente abzurufen, die für das Paket erforderlich/empfohlen sind, verwenden Sie die Optionen `--requires` und `--recommends`:

```
zypper info --requires MozillaFirefox
```

Das `what-provides-`*`Paket`* gleicht dem `rpm -q --whatprovides-`*`Paket`*, aber RPM ist nur für Abfragen der RPM-Datenbank (die Datenbank aller installierten Pakete) möglich. zypper informiert Sie auf der anderen Seite über Anbieter der Möglichkeit von einem beliebigen Repository, nicht nur von denen, die installiert sind.

7.1.7 Konfigurieren von Zypper

Zypper ist nunmehr mit einer Konfigurationsdatei ausgestattet, in der Sie die Arbeitsweise von Zypper dauerhaft verändern können (wahlweise systemweit oder benutzerspezifisch). Für systemweite Änderungen bearbeiten Sie `/etc/zypp/zypper.conf`. Für benutzerspezifische Änderungen bearbeiten Sie `~/.zypper.conf`. Falls `~/.zypper.conf` noch nicht vorhanden ist, können Sie `/etc/zypp/zypper.conf` als Schablone verwenden. Kopieren Sie diese Datei in `~/.zypper.conf` und passen Sie sie nach Ihren Anforderungen an. Weitere Informationen zu den verfügbaren Optionen finden Sie in den Kommentaren in der Datei.

7.1.8 Fehlersuche

Falls Probleme beim Zugriff auf Pakete von konfigurierten Repositorys auftreten (beispielsweise kann Zypper ein bestimmtes Paket nicht finden, obwohl Sie wissen, dass sich dieses Paket in einem der Repositorys befindet), kann schon das Aktualisieren der Repositorys Abhilfe bringen:

```
zypper refresh
```

Falls das nicht wirkt, probieren Sie Folgendes:

```
zypper refresh -fdb
```

Damit wird eine vollständige Aktualisierung und ein kompletter Neuaufbau der Datenbank erzwungen, außerdem ein erzwungener Download von Roh-Metadaten.

7.1.9 Zypper Rollback-Funktion im btrfs-Dateisystem

Wenn in der Root-Partition das btrfs-Dateisystem verwendet wird und `snapper` installiert ist, ruft zypper automatisch `snapper` auf (über ein von `snapper` installiertes Skript), wenn Änderungen des Dateisystems übermittelt werden, so dass entsprechende Dateisystem-Snapshots erstellt werden. Diese Snapshots können verwendet werden, um alle durch zypper vorgenommenen Änderungen rückgängig zu machen. Weitere Informationen zu `snapper`finden Sie unter `man snapper`.

zypper (und YaST) erstellen zurzeit nur Snapshots des Stamm-Dateisystems. Andere Subvolumes können nicht konfiguriert werden. Diese Funktion wird für das standardmäßige Dateisystem nicht unterstützt.

7.2 RPM - der Paket-Manager

RPM (RPM Package Manager) wird für die Verwaltung von Softwarepaketen verwendet. Seine Hauptbefehle lauten `rpm` und `rpmbuild`. In der leistungsstarken RPM-Datenbank können Benutzer, Systemadministratoren und Paketersteller ausführliche Informationen zur installierten Software abfragen.

Im Wesentlichen hat `rpm` fünf Modi: Installieren/Deinstallieren (oder Aktualisieren) von Software-Paketen, Neuaufbauen der RPM-Datenbank, Abfragen der RPM-Basis oder individuellen RPM-Archive, Integritätsprüfung der Pakete und Signieren von Paketen. `rpmbuild` ermöglicht das Aufbauen installierbarer Pakete von Pristine-Quellen.

Installierbare RPM-Archive sind in einem speziellen binären Format gepackt. Diese Archive bestehen aus den zu installierenden Programmdateien und aus verschiedenen Metadaten, die bei der Installation von `rpm` benutzt werden, um das jeweilige Softwarepaket zu konfigurieren, oder die zu Dokumentationszwecken in der RPM-Datenbank gespeichert werden. RPM-Archive haben für gewöhnlich die Dateinamenserweiterung `.rpm`.

TIPP: Pakete zur Software-Entwicklung

Bei etlichen Paketen sind die zur Software-Entwicklung erforderlichen Komponenten (Bibliotheken, Header- und Include-Dateien usw.) in eigene Pakete ausgelagert. Diese Entwicklungspakete werden nur benötigt, wenn Sie Software selbst kompilieren möchten (beispielsweise die neuesten GNOME-Pakete). Solche Pakete sind am Namenszusatz `-devel` zu erkennen, z. B. die Pakete `alsa-devel`, `gimp-devel` und `libkde4-develdevel`.

7.2.1 Prüfen der Authentizität eines Pakets

RPM-Pakete sind mit GPG signiert. Verifizieren Sie die Signatur eines RPM-Pakets mit dem Kommando `rpm --checksig` *`package`*`-1.2.3.rpm`. So können Sie feststellen, ob das Paket von Novell/SUSE oder einer anderen verbürgten Einrichtung stammt. Dies ist insbesondere bei Update-Paketen aus dem Internet zu empfehlen.

7.2.2 Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren

In der Regel kann ein RPM-Archiv einfach installiert werden: `rpm -i` *`package`*`.rpm`. Mit diesem Kommando wird das Paket aber nur dann installiert, wenn seine Abhängigkeiten erfüllt sind und keine Konflikte mit anderen Paketen bestehen. `rpm`fordert per Fehlermeldung die Pakete an, die zum Erfüllen der Abhängigkeiten installiert werden müssen. Im Hintergrund wacht die RPM-Datenbank darüber, dass keine Konflikte entstehen: Eine spezifische Datei darf nur zu einem Paket gehören. Durch die Wahl anderer Optionen können Sie `rpm` zwingen, diese Standards zu ignorieren, jedoch ist dies nur für Spezialisten gedacht. Andernfalls wird damit die Integrität des Systems gefährdet und möglicherweise die Update-Fähigkeit aufs Spiel gesetzt.

Die Optionen `-U` oder `--upgrade` und `-F` oder `--freshen` können für das Update eines Pakets benutzt werden (z. B.: `rpm -F` *`paket`*`.rpm`). Dieser Befehl entfernt die Dateien der alten Version und installiert sofort die neuen Dateien. Der Unterschied zwischen den beiden Versionen besteht darin, dass mit `-U` auch Pakete installiert werden, die vorher nicht im System vorhanden waren, wohingegen mit `-F` nur zuvor installierte Pakete aktualisiert werden. Bei einem Update verwendet `rpm` zur sorgfältigen Aktualisierung der Konfigurationsdateien die folgende Strategie:

- Falls eine Konfigurationsdatei vom Systemadministrator nicht geändert wurde, installiert `rpm` die neue Version der entsprechenden Datei. Es sind keine Eingriffe seitens des Administrators nötig.

- Falls eine Konfigurationsdatei vom Systemadministrator vor dem Update geändert wurde, speichert `rpm` die geänderte Datei mit der Erweiterung `.rpmorig` oder `.rpmsave` (Sicherungsdatei) und installiert nur dann die Version aus dem neuen Paket, wenn sich die ursprünglich installierte Datei und die neue Version unterscheiden. Vergleichen Sie in diesem Fall die Sicherungsdatei (`.rpmorig` oder `.rpmsave`) mit der neu installierten Datei und nehmen Sie Ihre Änderungen erneut in der neuen Datei vor. Löschen Sie anschließend unbedingt alle `.rpmorig`- und `.rpmsave`-Dateien, um Probleme mit zukünftigen Updates zu vermeiden.

- `.rpmnew`-Dateien erscheinen immer dann, wenn die Konfigurationsdatei bereits existiert *und* wenn die Kennung `noreplace` mit der `.spec`-Datei angegeben wurde.

Im Anschluss an ein Update sollten alle `.rpmsave`- und `.rpmnew`-Dateien nach einem Abgleich entfernt werden, damit sie bei zukünftigen Updates nicht stören. Die Erweiterung `.rpmorig` wird zugewiesen, wenn die Datei zuvor nicht von der RPM-Datenbank erkannt wurde.

Andernfalls wird `.rpmsave` verwendet. Mit anderen Worten: `.rpmorig` entsteht bei einem Update von einem Fremdformat auf RPM. `.rpmsave` entsteht bei einem Update aus einem älteren RPM auf einen neueren RPM. `.rpmnew` informiert nicht darüber, ob der Systemadministrator die Konfigurationsdatei geändert hat. Eine Liste all dieser Dateien ist in `/var/adm/rpmconfigcheck` verfügbar. Einige Konfigurationsdateien (wie `/etc/httpd/httpd.conf`) werden nicht überschrieben, um den weiteren Betrieb zu ermöglichen.

Der Schalter `-U` ist *nicht* einfach gleichbedeutend mit der Deinstallation mit der Option `-e` und der Installation mit der Option `-i`. Verwenden Sie `-U`, wann immer möglich.

Zum Entfernen eines Pakets geben Sie `rpm -e` *`paket`* ein. `rpm` löscht das Paket nur, wenn keine ungelösten Abhängigkeiten vorhanden sind. Theoretisch ist es unmöglich, beispielsweise Tcl/Tk zu löschen, solange eine andere Anwendung Tcl/Tk noch benötigt. Auch in diesem Fall nutzt RPM die Datenbank zur Unterstützung. Falls in einem Ausnahmefall ein solcher Löschvorgang nicht möglich ist (selbst wenn *keine*

Abhängigkeiten mehr bestehen), kann es nützlich sein, die RPM-Datenbank mit der Option `--rebuilddb` neu aufzubauen.

7.2.3 RPM und Patches

Um die Betriebssicherheit eines Systems zu garantieren, müssen von Zeit zu Zeit Update-Pakete auf dem System installiert werden. Bisher konnte ein Fehler in einem Paket nur eliminiert werden, indem das vollständige Paket ersetzt wurde. Umfangreiche Pakete mit Bugs in kleinen Dateien können leicht zu diesem Szenario führen. Jedoch bietet SUSE RPM nun eine Funktion, mit der Patches in Pakete installiert werden können.

Die wichtigsten Überlegungen dazu werden am Beispiel `pine` aufgezeigt:

Ist der Patch-RPM für mein System geeignet?

Um dies zu prüfen, fragen Sie zunächst die installierte Version des Pakets ab. Im Fall von `pine` verwenden Sie das Kommando:

```
rpm -q pine
pine-4.44-188
```

Prüfen Sie dann, ob der Patch-RPM sich für diese Version von `pine` eignet:

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

Dieser Patch passt zu drei verschiedenen Versionen von pine. Auch die im Beispiel installierte Version wird aufgeführt, d. h. der Patch kann installiert werden.

Welche Dateien werden durch den Patch ersetzt?

Die durch einen Patch betroffenen Dateien können leicht im Patch-RPM abgelesen werden. Der `rpm`-Parameter `-P` ermöglicht die Auswahl von speziellen Patch-Funktionen. Zeigen Sie die Dateiliste mit dem folgenden Befehl an:

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Oder verwenden Sie, falls der Patch bereits installiert ist, den folgenden Befehl:

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Wie kann ein Patch-RPM im System installiert werden?
: Patch-RPMs werden wie normale RPMs verwendet. Der einzige Unterschied liegt darin, dass ein passender RPM bereits installiert sein muss.

Welche Patches sind bereits auf dem System installiert und zu welchen Paketversionen gehören sie?
: Eine Liste aller im System installierter Patches kann über den Befehl `rpm -qPa` angezeigt werden. Wenn nur ein Patch in einem neuen System installiert ist (wie in unserem Beispiel), sieht die Liste wie folgt aus:

```
rpm -qPa
pine-4.44-224
```

Wenn Sie zu einem späteren Zeitpunkt wissen möchten, welche Paketversion ursprünglich installiert war, können Sie auch diese Information der RPM-Datenbank entnehmen. Für `pine` rufen Sie diese Information mit dem folgenden Befehl ab:

```
rpm -q --basedon pine
pine = 4.44-188
```

Weitere Informationen, auch zur Patch-Funktion von RPM, stehen auf den man-Seiten von `rpm` und `rpmbuild` zur Verfügung.

ANMERKUNG: Offizielle Aktualisierungen für SUSE Linux Enterprise Desktop

Damit die Download-Größe von Updates möglichst klein gehalten wird, werden offizielle Aktualisierungen für SUSE Linux Enterprise Desktop nicht als Patch-RPMs, sondern als Delta-RPM-Pakete zur Verfügung gestellt. Weitere Informationen finden Sie unter Abschnitt 7.2.4, „Delta-RPM-Pakete“ (S. 94).

7.2.4 Delta-RPM-Pakete

Delta-RPM-Pakete enthalten die Unterschiede zwischen einer alten und einer neuen Version eines RPM-Pakets. Wenn Sie ein Delta-RPM auf ein altes RPM anwenden, ergibt dies ein ganz neues RPM. Es ist nicht erforderlich, dass eine Kopie des alten RPM vorhanden ist, da ein Delta-RPM auch mit einem installierten RPM arbeiten kann.

Die Delta-RPM-Pakete sind sogar kleiner als Patch-RPMs, was beim Übertragen von Update-Paketen über das Internet von Vorteil ist. Der Nachteil ist, dass Update-Vorgänge mit Delta-RPMs erheblich mehr CPU-Zyklen beanspruchen als normale oder Patch-RPMs.

Die Binärdateien `prepdeltarpm`, `writedeltarpm` und `applydeltarpm` sind Teil der Delta-RPM-Suite (Paket `deltarpm`) und helfen Ihnen beim Erstellen und Anwenden von Delta-RPM-Paketen. Mit den folgenden Befehlen erstellen Sie ein Delta-RPM mit dem Namen `new.delta.rpm`. Der folgende Befehl setzt voraus, dass `old.rpm` und `new.rpm` vorhanden sind:

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

Entfernen Sie zum Schluss die temporären Arbeitsdateien `old.cpio`, `new.cpio` und `delta`.

Mit `applydeltarpm` können Sie den neuen RPM aus dem Dateisystem rekonstruieren, wenn das alte Paket bereits installiert ist:

```
applydeltarpm new.delta.rpm new.rpm
```

Um es aus dem alten RPM abzuleiten, ohne auf das Dateisystem zuzugreifen, verwenden Sie die Option `-r`:

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Technische Details finden Sie in `/usr/share/doc/packages/deltarpm/README`.

7.2.5 RPM Abfragen

Mit der Option `-q` initiiert `rpm` Abfragen und ermöglicht es, ein RPM-Archiv zu prüfen (durch Hinzufügen der Option `-p`) und auch die RPM-Datenbank nach installierten Paketen abzufragen. Zur Angabe der benötigten Informationsart stehen mehrere Schalter zur Verfügung. Weitere Informationen hierzu finden Sie unter Tabelle 7.1, „Die wichtigsten RPM-Abfrageoptionen“ (S. 96).

Tabelle 7.1 ***Die wichtigsten RPM-Abfrageoptionen***

`-i`	Paketinformation
`-l`	Dateiliste
`-f FILE`	Abfrage nach Paket, das die Datei *FILE* enthält. (*FILE* muss mit dem vollständigen Pfad angegeben werden.)
`-s`	Dateiliste mit Statusinformation (impliziert `-l`)
`-d`	Nur Dokumentationsdateien auflisten (impliziert `-l`)
`-c`	Nur Konfigurationsdateien auflisten (impliziert `-l`)
`--dump`	Dateiliste mit vollständigen Details (mit `-l`, `-c` oder `-d` benutzen)
`--provides`	Funktionen des Pakets auflisten, die ein anderes Paket mit `--requires` anfordern kann
`--requires`, `-R`	Fähigkeiten, die das Paket benötigt
`--Skripten`	Installationsskripten (preinstall, postinstall, uninstall)

Beispielsweise gibt der Befehl `rpm -q -i wget` die in Beispiel 7.2, „rpm -q -i wget" (S. 96) gezeigte Information aus.

Beispiel 7.2 *rpm -q -i wget*

```
Name        : wget                         Relocations: (not relocatable)
Version     : 1.11.4                            Vendor: openSUSE
Release     : 1.70                          Build Date: Sat 01 Aug 2009
09:49:48 CEST
Install Date: Thu 06 Aug 2009 14:53:24 CEST      Build Host: build18
Group       : Productivity/Networking/Web/Utilities   Source RPM:
```

```
wget-1.11.4-1.70.src.rpm
Size        : 1525431                          License: GPL v3 or later
Signature   : RSA/8, Sat 01 Aug 2009 09:50:04 CEST, Key ID b88b2fd43dbdc284
Packager    : http://bugs.opensuse.org
URL         : http://www.gnu.org/software/wget/
Summary     : A Tool for Mirroring FTP and HTTP Servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

Die Option `-f` funktioniert nur, wenn Sie den kompletten Dateinamen mit dem vollständigen Pfad angeben. Sie können so viele Dateinamen wie nötig angeben. Beispielsweise führt der folgende Befehl

```
rpm -q -f /bin/rpm /usr/bin/wget
```

zum Ergebnis:

```
rpm-4.8.0-4.3.x86_64
wget-1.11.4-11.18.x86_64
```

Wenn nur ein Teil des Dateinamens bekannt ist, verwenden Sie ein Shell-Skript, wie in Beispiel 7.3, „Skript für die Suche nach Paketen" (S. 97) gezeigt. Übergeben Sie den partiellen Dateinamen als Parameter beim Aufruf des Skripts.

Beispiel 7.3 *Skript für die Suche nach Paketen*

```
#! /bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

Das Kommando `rpm -q --changelog rpm` zeigt eine detaillierte Liste der Änderungsinformation zu einem bestimmten Paket (in diesem Fall das `rpm`-Paket) nach Datum sortiert an.

Mithilfe der installierten RPM-Datenbank sind Überprüfungen möglich. Leiten Sie die Überprüfungen mit `-V`, `-y` oder `--verify` ein. Mit dieser Option zeigt `rpm` alle Dateien in einem Paket an, die seit der Installation geändert wurden. `rpm` verwendet acht verschiedene Zeichen als Hinweis auf die folgenden Änderungen:

Tabelle 7.2 *RPM-Überprüfungsoptionen*

`5`	MD5-Prüfsumme

S	Dateigröße
L	Symbolischer Link
T	Änderungszeit
D	Major- und Minor-Gerätenummern
U	Eigentümer
G	Gruppe
M	Modus (Berechtigungen und Dateityp)

Bei Konfigurationsdateien wird der Buchstabe c ausgegeben. Beispielsweise für Änderungen an /etc/wgetrc (wget-Paket):

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Die Dateien der RPM-Datenbank werden in /var/lib/rpm abgelegt. Wenn die Partition /usr eine Größe von 1 GB aufweist, kann diese Datenbank beinahe 30 MB belegen, insbesondere nach einem kompletten Update. Wenn die Datenbank viel größer ist als erwartet, kann es nützlich sein, die Datenbank mit der Option --rebuilddb neu zu erstellen. Legen Sie zuvor eine Sicherungskopie der alten Datenbank an. Das cron-Skript cron.daily legt täglich (mit gzip gepackte) Kopien der Datenbank an und speichert diese unter /var/adm/backup/rpmdb. Die Anzahl der Kopien wird durch die Variable MAX_RPMDB_BACKUPS (Standard: 5) in /etc/sysconfig/backup gesteuert. Die Größe einer einzelnen Sicherungskopie beträgt ungefähr 1 MB für 1 GB in /usr.

7.2.6 Installieren und Kompilieren von Quellpaketen

Alle Quellpakete haben die Erweiterung .src.rpm (Source-RPM).

ANMERKUNG: Installierte Quellpakete

Quellpakete können vom Installationsmedium auf die Festplatte kopiert und mit YaST entpackt werden. Sie werden im Paket-Manager jedoch nicht als installiert (`[i]`) gekennzeichnet. Das liegt daran, dass die Quellpakete nicht in der RPM-Datenbank eingetragen sind. Nur *installierte* Betriebssystemsoftware wird in der RPM-Datenbank aufgeführt. Wenn Sie ein Quellpaket „installieren", wird dem System nur der Quellcode hinzugefügt.

Die folgenden Verzeichnisse müssen für `rpm` und `rpmbuild` in `/usr/src/packages` vorhanden sein (es sei denn, Sie haben spezielle Einstellungen in einer Datei, wie `/etc/rpmrc`, festgelegt):

`SOURCES`
: für die originalen Quellen (`.tar.bz2` oder `.tar.gz` files, etc.) und für die distributionsspezifischen Anpassungen (meistens `.diff`- oder `.patch`-Dateien)

`SPECS`
: für die `.spec`-Dateien, die ähnlich wie Meta-Makefiles den *build*-Prozess steuern

`BUILD`
: Alle Quellen in diesem Verzeichnis werden entpackt, gepatcht und kompiliert.

`RPMS`
: Speicherort der fertigen Binärpakete

`SRPMS`
: Speicherort der Quell-RPMs

Wenn Sie ein Quellpaket mit YaST installieren, werden alle erforderlichen Komponenten in `/usr/src/packages` installiert: die Quellen und Anpassungen in `SOURCES` und die relevante `.spec`-Datei in `SPECS`.

WARNUNG

Experimentieren Sie nicht mit Systemkomponenten (`glibc`, `rpm`, `sysvinit` usw.), da Sie damit die Stabilität Ihres Systems aufs Spiel setzen.

Das folgende Beispiel verwendet das `wget.src.rpm`-Paket. Nach der Installation des Quellpakets sollten Dateien wie in der folgenden Liste vorhanden sein:

```
/usr/src/packages/SOURCES/wget-1.11.4.tar.bz2
/usr/src/packages/SOURCES/wgetrc.patch
/usr/src/packages/SPECS/wget.spec
```

Mit `rpmbuild -b X /usr/src/packages/SPECS/wget.spec` wird die Kompilierung gestartet. *X* ist ein Platzhalter für verschiedene Stufen des build-Prozesses (Einzelheiten siehe in `--help` oder der RPM-Dokumentation). Nachfolgend wird nur eine kurze Erläuterung gegeben:

`-bp`
: Bereiten Sie Quellen in `/usr/src/packages/BUILD` vor: entpacken und patchen.

`-bc`
: Wie `-bp`, jedoch zusätzlich kompilieren.

`-bi`
: Wie `-bp`, jedoch zusätzlich die erstellte Software installieren. Vorsicht: Wenn das Paket die Funktion BuildRoot nicht unterstützt, ist es möglich, dass Konfigurationsdateien überschrieben werden.

`-bb`
: Wie `-bi`, jedoch zusätzlich das Binärpaket erstellen. Nach erfolgreicher Kompilierung sollte das Binärpaket in `/usr/src/packages/RPMS` sein.

`-ba`
: Wie `-bb`, jedoch zusätzlich den Quell-RPM erstellen. Nach erfolgreicher Kompilierung sollte dieses in `/usr/src/packages/RPMS` liegen.

`--short-circuit`
: Einige Schritte überspringen.

Der erstellte Binär-RPM kann nun mit `rpm -i` oder vorzugsweise mit `rpm -U` erstellt werden. Durch die Installation mit `rpm` wird er in die RPM-Datenbank aufgenommen.

7.2.7 Kompilieren von RPM-Pakten mit „build“

Bei vielen Paketen besteht die Gefahr, dass während der Erstellung ungewollt Dateien in das laufende System kopiert werden. Um dies zu vermeiden, können Sie `build` verwenden, das eine definierte Umgebung herstellt, in der das Paket erstellt wird. Zum Aufbau dieser chroot-Umgebung muss dem `build`-Skript ein kompletter Paketbaum zur Verfügung stehen. Dieser kann auf Festplatte, über NFS oder auch von DVD bereitgestellt werden. Legen Sie die Position mit `build --rpms` *`Verzeichnis`* fest. Im Unterschied zu `rpm` sucht das Kommando `build` die `-spec`-Datei im Quellverzeichnis. Wenn Sie, wie im obigen Beispiel, `wget` neu erstellen möchten und die DVD unter `/media/dvd` im System eingehängt ist, verwenden Sie als Benutzer `root` folgende Kommandos:

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Anschließend wird in `/var/tmp/build-root` eine minimale Umgebung eingerichtet. Das Paket wird in dieser Umgebung erstellt. Danach befinden sich die resultierenden Pakete in `/var/tmp/build-root/usr/src/packages/RPMS`.

Das `build`-Skript bietet eine Reihe zusätzlicher Optionen. Beispielsweise können Sie das Skript veranlassen, Ihre eigenen RPMs bevorzugt zu verwenden, die Initialisierung der build-Umgebung auszulassen oder das Kommando `rpm` auf eine der oben erwähnten Stufen zu beschränken. Weitere Informationen erhalten Sie über `build --help` oder die man-Seite `build`.

7.2.8 Werkzeuge für RPM-Archive und die RPM-Datenbank

Midnight Commander (`mc`) kann den Inhalt von RPM-Archiven anzeigen und Teile daraus kopieren. Archive werden als virtuelle Dateisysteme dargestellt und bieten alle üblichen Menüoptionen von Midnight Commander. Zeigen Sie den `HEADER` mit F3 an. Zeigen Sie die Archivstruktur mit den Cursortasten und der Eingabetaste an. Kopieren Sie Archivkomponenten mit F5.

Ein Paket-Manager mit allen Funktionen ist als YaST-Modul verfügbar. Weitere Informationen finden Sie unter Kapitel 6, *Installieren bzw. Entfernen von Software* (↑*Bereitstellungshandbuch*).

8 Bash-Shell und Bash-Skripte

Heutzutage werden zunehmend Computer mit einer grafischen Benutzeroberfläche (GUI) wie KDE oder GNOME verwendet. Diese bieten zwar viele Funktionen, jedoch ist ihre Verwendung beschränkt, was automatisierte Aufgaben angeht. Shells sind eine gute Ergänzung für GUIs, und dieses Kapitel gibt Ihnen einen Überblick über einige Aspekte von Shells, in diesem Fall die Bash-Shell.

8.1 Was ist „die Shell“?

Traditionell handelt es sich bei *der* Shell um Bash (Bourne again Shell). Wenn in diesem Kapitel die Rede von „der Shell“ ist, ist die Bash-Shell gemeint. Außer Bash sind noch weitere Shells verfügbar (ash, csh, ksh, zsh und viele mehr), von denen jede unterschiedliche Funktionen und Merkmale aufweist. Wenn Sie weitere Informationen über andere Shells wünschen, suchen Sie in YaST nach *shell*.

8.1.1 Die Bash-Konfigurationsdateien

Eine Shell lässt sich aufrufen als:

1. **Interaktive Login-Shell** Diese wird zum Anmelden bei einem Computer durch den Aufruf von Bash mit der Option `--login` verwendet oder beim Anmelden an einem entfernten Computer mit SSH.

2. **„Gewöhnliche“ interaktive Shell** Dies ist normalerweise beim Starten von xterm, konsole, gnome-terminal oder ähnlichen Tools der Fall.

3. **Nicht interaktive Shell** Dies wird beim Aufrufen eines Shell-Skripts in der Kommandozeile verwendet.

Abhängig vom verwendeten Shell-Typ werden unterschiedliche Konfigurationsdateien gelesen. Die folgenden Tabellen zeigen die Login- und Nicht-Login-Shell-Konfigurationsdateien.

Tabelle 8.1 *Bash-Konfigurationsdateien für Login-Shells*

Datei	Beschreibung
`/etc/profile`	Bearbeiten Sie diese Datei nicht, andernfalls können Ihre Änderungen bei Ihrem nächsten Update zerstört werden.
`/etc/profile.local`	Verwenden Sie diese Datei, wenn Sie `/etc/profile` erweitern.
`/etc/profile.d/`	Enthält systemweite Konfigurationsdateien für bestimmte Programme
`~/.profile`	Fügen Sie hier benutzerspezifische Konfigurationsdaten für Login-Shells ein.

Tabelle 8.2 *Bash-Konfigurationsdateien für Nicht-Login-Shells*

`/etc/bash.bashrc`	Bearbeiten Sie diese Datei nicht, andernfalls können Ihre Änderungen bei Ihrem nächsten Update zerstört werden.
`/etc/bash.bashrc.local`	Verwenden Sie diese Datei, um Ihre systemweiten Änderungen nur für die Bash-Shell einzufügen.
`~/.bashrc`	Fügen Sie hier benutzerspezifische Konfigurationsdaten ein.

Daneben verwendet die Bash-Shell einige weitere Dateien:

Tabelle 8.3 *Besondere Dateien für die Bash-Shell*

Datei	Beschreibung
`~/.bash_history`	Enthält eine Liste aller Kommandos, die Sie eingegeben haben.
`~/.bash_logout`	Wird beim Abmelden ausgeführt.

8.1.2 Die Verzeichnisstruktur

Die folgende Tabelle bietet eine kurze Übersicht über die wichtigsten Verzeichnisse der höheren Ebene auf einem Linux-System. Ausführlichere Informationen über die Verzeichnisse und wichtige Unterverzeichnisse erhalten Sie in der folgenden Liste.

Tabelle 8.4 *Überblick über eine Standardverzeichnisstruktur*

Verzeichnis	Inhalt
`/`	Root-Verzeichnis – Startpunkt der Verzeichnisstruktur.
`/bin`	Grundlegende binäre Dateien, z. B. Kommandos, die der Systemadministrator und normale Benutzer brauchen. Enthält gewöhnlich auch die Shells, z. B. Bash.
`/boot`	Statische Dateien des Bootloaders.
`/dev`	Erforderliche Dateien für den Zugriff auf Host-spezifische Geräte.
`/etc`	Host-spezifische Systemkonfigurationsdateien.

Verzeichnis	Inhalt
/home	Enthält die Home-Verzeichnisse aller Benutzer mit einem Konto im System. Das Home-Verzeichnis von root befindet sich jedoch nicht unter /home, sondern unter /root.
/lib	Grundlegende freigegebene Bibliotheken und Kernel-Module.
/media	Einhängepunkte für Wechselmedien.
/mnt	Einhängepunkt für das temporäre Einhängen eines Dateisystems.
/opt	Add-On-Anwendungssoftwarepakete.
/root	Home-Verzeichnis für den Superuser root.
/sbin	Grundlegende Systembinärdateien.
/srv	Daten für Dienste, die das System bereitstellt.
/tmp	Temporäre Dateien.
/usr	Sekundäre Hierarchie mit Nur-Lese-Daten.
/var	Variable Daten wie Protokolldateien.
/windows	Nur verfügbar, wenn sowohl Microsoft Windows* als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten.

Die folgende Liste bietet detailliertere Informationen und einige Beispiele für die Dateien und Unterverzeichnisse, die in den Verzeichnissen verfügbar sind:

`/bin`
: Enthält die grundlegenden Shell-Befehle, die `root` und andere Benutzer verwenden können. Zu diesen Kommandos gehören `ls`, `mkdir`, `cp`, `mv`, `rm` und `rmdir`. `/bin` umfasst außerdem Bash, die Standard-Shell in SUSE Linux Enterprise Desktop.

`/boot`
: Enthält Daten, die zum Booten erforderlich sind, wie zum Beispiel den Bootloader, den Kernel und andere Daten, die verwendet werden, bevor der Kernel mit der Ausführung von Programmen im Benutzermodus beginnt.

`/dev`
: Enthält Gerätedateien, die Hardware-Komponenten darstellen.

`/etc`
: Enthält lokale Konfigurationsdateien, die den Betrieb von Programmen wie das X Window System steuern können. Das Unterverzeichnis `/etc/init.d` enthält Skripten, die während des Bootvorgangs ausgeführt werden.

`/home/`*`Benutzername`*
: Enthält die privaten Daten aller Benutzer, die ein Konto auf dem System haben. Die Dateien, die hier gespeichert sind, können nur durch den Besitzer oder den Systemadministrator geändert werden. Standardmäßig befinden sich hier Ihr E-Mail-Verzeichnis und Ihre persönliche Desktopkonfiguration in Form von verborgenen Dateien und Verzeichnissen. KDE-Benutzer finden die persönlichen Konfigurationsdaten für Ihren Desktop unter `.kde4`, GNOME-Benutzer finden sie unter `.gconf`.

ANMERKUNG: Home-Verzeichnis in einer Netzwerkumgebung

Wenn Sie in einer Netzwerkumgebung arbeiten, kann Ihr Home-Verzeichnis einem von `/home` abweichenden Verzeichnis zugeordnet sein.

`/lib`
: Enthält die grundlegenden freigegebenen Bibliotheken, die zum Booten des Systems und zur Ausführung der Kommandos im Root-Dateisystem erforderlich sind. Freigegebene Bibliotheken entsprechen in Windows DLL-Dateien.

`/media`
: Enthält Einhängepunkte für Wechselmedien, wie zum Beispiel CD-ROMs, USB-Sticks und Digitalkameras (sofern sie USB verwenden). Unter `/media` sind beliebige Laufwerktypen gespeichert, mit Ausnahme der Festplatte Ihres Systems. Sobald Ihr Wechselmedium eingelegt bzw. mit dem System verbunden und eingehängt wurde, können Sie von hier darauf zugreifen.

`/mnt`
: Dieses Verzeichnis bietet einen Einhängepunkt für ein vorübergehend eingehängtes Dateisystem. `root` kann hier Dateisysteme einhängen.

`/opt`
: Reserviert für die Installation von Drittanbieter-Software. Hier finden Sie optionale Softwareprogramme und größere Add-On-Programmpakete.

`/root`
: Home-Verzeichnis für den Benutzer `root`. Hier befinden sich die persönlichen Daten von `root`.

`/sbin`
: Wie durch das `s` angegeben, enthält dieses Verzeichnis Dienstprogramme für den Superuser. `/sbin` enthält die Binärdateien, die zusätzlich zu den Binärdateien in `/bin` zum Booten und Wiederherstellen des Systems unbedingt erforderlich sind.

`/srv`
: Enhält Daten für Dienste, die das System bereitstellt, z. B. FTP und HTTP.

`/tmp`
: Dieses Verzeichnis wird von Programmen benutzt, die eine temporäre Speicherung von Dateien verlangen.

WICHTIG: Bereinigen des temporären Verzeichnisses `/tmp` bei Systemstart

Im Verzeichnis `/tmp` gespeicherte Daten werden nicht zwingend bei einem Neustart des Systems beibehalten. Dies hängt zum Beispiel von den Einstellungen unter `/etc/sysconfig/cron` ab.

`/usr`
: `/usr` hat nichts mit Benutzern („user") zu tun, sondern ist das Akronym für UNIX-Systemressourcen. Die Daten in `/usr` sind statische, schreibgeschützte Daten, die auf verschiedenen Hosts freigegeben sein können, die den Filesystem Hierarchy Standard (FHS) einhalten. Dieses Verzeichnis enthält alle Anwendungsprogramme und bildet eine sekundäre Hierarchie im Dateisystem. Dort befinden sich auch KDE4 und GNOME. `/usr` enthält eine Reihe von Unterverzeichnissen, z. B. `/usr/bin`, `/usr/sbin`, `/usr/local` und `/usr/share/doc`.

`/usr/bin`
: Enthält Programme, die für den allgemeinen Zugriff verfügbar sind.

`/usr/sbin`
: Enthält Programme, die für den Systemadministrator reserviert sind, z. B. Reparaturfunktionen.

`/usr/local`
: In diesem Verzeichnis kann der Systemadministrator lokale, verteilungsunabhängige Erweiterungen installieren.

`/usr/share/doc`
: Enthält verschiedene Dokumentationsdateien und die Versionshinweise für Ihr System. Im Unterverzeichnis `Handbuch` befindet sich eine Online-Version dieses Handbuchs. Wenn mehrere Sprachen installiert sind, kann dieses Verzeichnis die Handbücher für verschiedene Sprachen enthalten.

  Im Verzeichnis `packages` finden Sie die Dokumentation zu den auf Ihrem System installierten Software-Paketen. Für jedes Paket wird ein Unterverzeichnis `/usr/share/doc/packages/`*`Paketname`* angelegt, das häufig README-Dateien für das Paket und manchmal Beispiele, Konfigurationsdateien oder zusätzliche Skripten umfasst.

Wenn HOWTOs (Verfahrensbeschreibungen) auf Ihrem System installiert sind, enhält `/usr/share/doc` auch das Unterverzeichnis `howto` mit zusätzlicher Dokumentation zu vielen Aufgaben im Zusammenhang mit der Einrichtung und Ausführung von Linux-Software.

`/var`
Während `/usr` statische, schreibgeschützte Daten enthält, ist `/var` für Daten, die während des Systembetriebs geschrieben werden und daher variabel sind, z. B. Protokolldateien oder Spooling-Daten. Eine Übersicht über die wichtigsten Protokolldateien finden Sie unter `/var/log/`. Weitere Informationen stehen unter Tabelle 31.1, „Protokolldateien“ (S. 458) zur Verfügung.

`/windows`
Nur verfügbar, wenn sowohl Microsoft Windows als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten, die auf der Windows-Partition Ihres Systems verfügbar sind. Ob Sie die Daten in diesem Verzeichnis bearbeiten können, hängt vom Dateisystem ab, das Ihre Windows-Partition verwendet. Falls es sich um FAT32 handelt, können Sie die Dateien in diesem Verzeichnis öffnen und bearbeiten. Für NTFS unterstützt SUSE Linux Enterprise Desktop auch den Schreibzugriff. Die Funktionalität des Treibers für das NTFS-3g-Dateisystem ist jedoch eingeschränkt. .

8.2 Schreiben von Shell-Skripten

Shell-Skripte bieten eine bequeme Möglichkeit, alle möglichen Aufgaben zu erledigen: Erfassen von Daten, Suche nach einem Wort oder Begriff in einem Text und viele andere nützliche Dinge. Das folgende Beispiel zeigt ein kleines Shell-Skript, das einen Text druckt:

Beispiel 8.1 *Ein Shell-Skript, das einen Text druckt*

```
#!/bin/sh ❶
# Output the following line: ❷
echo "Hello World" ❸
```

❶ Die erste Zeile beginnt mit dem *Shebang* -Zeichen (`#!`), das darauf hinweist, dass es sich bei dieser Datei um ein Skript handelt. Das Skript wird mit dem Interpreter ausgeführt, der nach dem Shebang angegeben ist, in diesem Fall mit `/bin/sh`.

❷ Die zweite Zeile ist ein Kommentar, der mit dem Hash-Zeichen beginnt. Es wird empfohlen, schwierige Zeilen zu kommentieren, damit ihre Bedeutung auch später klar ist.

❸ Die dritte Zeile verwendet das integrierte Kommando `echo`, um den entsprechenden Text zu drucken.

Bevor Sie dieses Skript ausführen können, müssen einige Voraussetzungen erfüllt sein:

1. Jedes Skript muss eine Shebang-Zeile enthalten. (Dies ist im obigen Beispiel bereits der Fall.) Wenn ein Skript diese Zeile nicht enthält, müssen Sie den Interpreter manuell aufrufen.

2. Sie können das Skript an beliebiger Stelle speichern. Jedoch empfiehlt es sich, es in einem Verzeichnis zu speichern, in dem die Shell es finden kann. Der Suchpfad in einer Shell wird durch die Umgebungsvariable `PATH` bestimmt. In der Regel verfügt ein normaler Benutzer über keinen Schreibzugriff auf `/usr/bin`. Daher sollten Sie Ihre Skripten im Benutzerverzeichnis `~/bin/` speichern. Das obige Beispiel erhält den Namen `hello.sh`.

3. Das Skript muss zum Ausführen von Dateien berechtigt sein. Stellen Sie die Berechtigungen mit dem folgenden Kommando ein:

   ```
   chmod +x ~/bin/hello.sh
   ```

Wenn Sie alle oben genannten Voraussetzungen erfüllt haben, können Sie das Skript mithilfe der folgenden Methoden ausführen:

1. **Als absoluten Pfad** Das Skript kann mit einem absoluten Pfad ausgeführt werden. In unserem Fall lautet er `~/bin/hello.sh`.

2. **Überall** Wenn die Umgebungsvariable `PATH` das Verzeichnis enthält, in dem sich das Skript befindet, können Sie das Skript einfach mit `hello.sh` ausführen.

8.3 Umlenken von Kommandoereignissen

Jedes Kommando kann drei Kanäle für Eingabe oder Ausgabe verwenden:

- **Standardausgabe** Dies ist der Standardausgabe-Kanal. Immer wenn ein Kommando eine Ausgabe erzeugt, verwendet es den Standardausgabe-Kanal.
- **Standardeingabe** Wenn ein Kommando Eingaben von Benutzern oder anderen Kommandos benötigt, verwendet es diesen Kanal.
- **Standardfehler** Kommandos verwenden diesen Kanal zum Melden von Fehlern.

Zum Umlenken dieser Kanäle bestehen folgende Möglichkeiten:

`Kommando > Datei`

Speichert die Ausgabe des Kommandos in eine Datei; eine etwaige bestehende Datei wird gelöscht. Beispielsweise schreibt das Kommando `ls` seine Ausgabe in die Datei `listing.txt`:

```
ls > listing.txt
```

`Kommando >> Datei`

Hängt die Ausgabe des Kommandos an eine Datei an. Beispielsweise hängt das Kommando `ls` seine Ausgabe an die Datei `listing.txt` an:

```
ls >> listing.txt
```

`Kommando < Datei`

Liest die Datei als Eingabe für das angegebene Kommando. Beispielsweise liest das Kommando `read` den Inhalt der Datei in die Variable ein:

```
read a < foo
```

`Kommando1 | Kommando2`

Leitet die Ausgabe des linken Kommandos als Eingabe für das rechte Kommando um. Beispiel: Das Kommando `cat` gibt den Inhalt der Datei `/proc/cpuinfo` aus. Diese Ausgabe wird von `grep` verwendet, um nur diejenigen Zeilen herauszufiltern, die `cpu` enthalten:

```
cat /proc/cpuinfo | grep cpu
```

Jeder Kanal verfügt über einen *Dateideskriptor*: 0 (Null) für Standardeingabe, 1 für Standardausgabe und 2 für Standardfehler. Es ist zulässig, diesen Dateideskriptor vor einem <- oder >-Zeichen einzufügen. Beispielsweise sucht die folgende Zeile nach einer Datei, die mit `foo` beginnt, aber seine Fehlermeldungen durch Umlenkung zu `/dev/null` unterdrückt:

```
find / -name "foo*" 2>/dev/null
```

8.4 Verwenden von Aliassen

Ein Alias ist ein Definitionskürzel für einen oder mehrere Kommandos. Die Syntax für einen Alias lautet:

```
alias NAME=DEFINITION
```

Beispielsweise definiert die folgende Zeile den Alias `lt`, der eine lange Liste ausgibt (Option `-l`), sie nach Änderungszeit sortiert (`-t`) und sie bei der Sortierung in umgekehrter Reihenfolge ausgibt (`-r`):

```
alias lt='ls -ltr'
```

Zur Anzeige aller Aliasdefinitionen verwenden Sie `alias`. Entfernen Sie den Alias mit `Alias entfernen` und dem entsprechenden Aliasnamen.

8.5 Verwenden von Variablen in der Bash-Shell

Eine Shell-Variable kann global oder lokal sein. Auf globale Variablen, z. B. Umgebungsvariablen, kann in allen Shells zugegriffen werden. Lokale Variablen sind hingegen nur in der aktuellen Shell sichtbar.

Verwenden Sie zur Anzeige von allen Umgebungsvariablen das Kommando `printenv`. Wenn Sie den Wert einer Variable kennen müssen, fügen Sie den Namen Ihrer Variablen als ein Argument ein:

```
printenv PATH
```

Eine Variable (global oder lokal) kann auch mit `echo` angezeigt werden:

```
echo $PATH
```

Verwenden Sie zum Festlegen einer lokalen Variablen einen Variablennamen, gefolgt vom Gleichheitszeichen und dem Wert für den Namen:

```
PROJECT="SLED"
```

Geben Sie keine Leerzeichen um das Gleichheitszeichen ein, sonst erhalten Sie einen Fehler. Verwenden Sie zum Setzen einer Umgebungsvariablen `export`:

```
export NAME="tux"
```

Zum Entfernen einer Variable verwenden Sie `unset`:

```
unset NAME
```

Die folgende Tabelle enthält einige häufige Umgebungsvariablen, die Sie in Ihren Shell-Skripten verwenden können:

Tabelle 8.5 *Nützliche Umgebungsvariablen*

`HOME`	Home-Verzeichnis des aktuellen Benutzers
`HOST`	Der aktuelle Hostname
`LANG`	Wenn ein Werkzeug lokalisiert wird, verwendet es die Sprache aus dieser Umgebungsvariablen. Englisch kann auch auf `C` gesetzt werden
`PFAD`	Suchpfad der Shell, eine Liste von Verzeichnissen, die durch Doppelpunkte getrennt sind
`PS1`	Gibt die normale Eingabeaufforderung an, die vor jedem Kommando angezeigt wird
`PS2`	Gibt die sekundäre Eingabeaufforderung an, die beim Ausführen eines mehrzeiligen Kommandos angezeigt wird
`PWD`	Aktuelles Arbeitsverzeichnis
`USER`	Aktueller Benutzer

8.5.1 Verwenden von Argumentvariablen

Wenn Sie beispielsweise über das Skript `foo.sh` verfügen, können Sie es wie folgt ausführen:

```
foo.sh "Tux Penguin" 2000
```

Für den Zugriff auf alle Argumente, die an Ihr Skript übergeben werden, benötigen Sie Positionsparameter. Diese sind `$1` für das erste Argument, `$2` für das zweite usw. Sie können bis zu neun Parameter verwenden. Verwenden Sie `$0` zum Abrufen des Skriptnamens.

Das folgende Skript `foo.sh` gibt alle Argumente von 1 bis 4 aus:

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

Wenn Sie das Skript mit den obigen Argumenten ausführen, erhalten Sie Folgendes:

```
"Tux Penguin" "2000" "" ""
```

8.5.2 Verwenden der Variablenersetzung

Variablenersetzungen wenden beginnend von links oder rechts ein Schema auf den Inhalt einer Variable an. Die folgende Liste enthält die möglichen Syntaxformen:

`${VAR#schema}`
: entfernt die kürzeste mögliche Übereinstimmung von links:

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##schema}`
: entfernt die längste mögliche Übereinstimmung von links:

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

`${VAR%schema}`
: entfernt die kürzeste mögliche Übereinstimmung von rechts:

```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%schema}`
: entfernt die längste mögliche Übereinstimmung von rechts:

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

`${VAR/pattern_1/pattern_2}`
: ersetzt den Inhalt von *`VAR`* von *`pattern_1`* durch *`pattern_2`*:

```
file=/home/tux/book/book.tar.bz2
echo ${file/tux/wilber}
/home/wilber/book/book.tar.bz2
```

8.6 Gruppieren und Kombinieren von Kommandos

In Shells können Sie Kommandos für die bedingte Ausführung verketten und gruppieren. Jedes Kommando übergibt einen Endcode, der den Erfolg oder Misserfolg seiner Ausführung bestimmt. Wenn er 0 (Null) lautet, war das Kommando erfolgreich, alle anderen Codes bezeichnen einen Fehler, der spezifisch für das Kommando ist.

Die folgende Liste zeigt, wie sich Kommandos gruppieren lassen:

`Kommando1 ; Kommando2`
: führt die Kommandos in sequenzieller Reihenfolge aus. Der Endcode wird nicht geprüft. Die folgende Zeile zeigt den Inhalt der Datei mit `cat` an und gibt deren Dateieigenschaften unabhängig von deren Endcodes mit `ls` aus:

```
cat filelist.txt ; ls -l filelist.txt
```

`Kommando1 && Kommando2`
: führt das rechte Kommando aus, wenn das linke Kommando erfolgreich war (logisches UND). Die folgende Zeile zeigt den Inahlt der Datei an und gibt deren Dateieigenschaften nur aus, wenn das vorherige Kommando erfolgreich war (vgl. mit dem vorherigen Eintrag in dieser Liste):

```
cat filelist.txt && ls -l filelist.txt
```

`Kommando1 || Kommando2`
: führt das rechte Kommando aus, wenn das linke Kommando fehlgeschlagen ist (logisches ODER). Die folgende Zeile legt nur ein Verzeichnis in `/home/wilber/bar` an, wenn die Erstellung des Verzeichnisses in `/home/tux/foo` fehlgeschlagen ist:

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

`funcname(){ ... }`
: erstellt eine Shell-Funktion. Sie können mithilfe der Positionsparameter auf ihre Argumente zugreifen. Die folgende Zeile definiert die Funktion `hello` für die Ausgabe einer kurzen Meldung:

```
hello() { echo "Hello $1"; }
```

Sie können diese Funktion wie folgt aufrufen:

```
hello Tux
```

Die Ausgabe sieht wie folgt aus:

```
Hello Tux
```

8.7 Arbeiten mit häufigen Ablaufkonstrukten

Zur Steuerung des Ablaufs Ihres Skripts verfügt eine Shell über `while`-, `if`-, `for`- und `case`-Konstrukte.

8.7.1 Das Steuerungskommando „if"

Das Kommando `if` wird verwendet, um Ausdrücke zu prüfen. Beispielsweise testet der folgende Code, ob es sich beim aktuellen Benutzer um Tux handelt:

```
if test $USER = "tux"; then
  echo "Hello Tux."
else
  echo "You are not Tux."
fi
```

Der Testausdruck kann so komplex oder einfach wie möglich sein. Der folgende Ausdruck prüft, ob die Datei `foo.txt` existiert:

```
if test -e /tmp/foo.txt ;
then
  echo "Found foo.txt"
fi
```

Der Testausdruck kann auch in eckigen Klammern abgekürzt werden:

```
if [ -e /tmp/foo.txt ] ; then
  echo "Found foo.txt"
fi
```

Weitere nützliche Ausdrücke finden Sie unter http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lsst/ch03sec02.html.

8.7.2 Erstellen von Schleifen mit dem Kommando "for"

Mithilfe der `for`-Schleife können Sie Kommandos an einer Liste von Einträgen ausführen. Beispielsweise gibt der folgende Code einige Informationen über PNG-Dateien im aktuellen Verzeichnis aus:

```
for i in *.png; do
 ls -l $i
done
```

8.8 Weiterführende Informationen

Wichtige Informationen über die Bash-Shell finden Sie auf den man-Seiten zu `man bash`. Für weitere Informationen zu diesem Thema siehe die folgende Liste:

- http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html – Bash Guide for Beginners (Bash-Anleitungen für Anfänger)
- http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html – BASH Programming - Introduction HOW-TO (BASH-Programmierung – Einführende schrittweise Anleitungen)

- http://tldp.org/LDP/abs/html/index.html – Advanced Bash-Scripting Guide (Anleitung für erweiterte Bash-Skripts)
- http://www.grymoire.com/Unix/Sh.html – Sh - the Bourne Shell (Sh – die Bourne-Shell)



9 Using Third-Party Software

For information about using third-party software installed on SUSE Linux Enterprise and support of SUSE products used with third-party software, see the following links:

SUSE Partner Engineering Services Partner Certification Support Agreement
: https://www.suse.com/partners/ihv/yes/partner_engineering_services.html

Partner Software Catalog
: https://www.suse.com/susePSC/home

YES Certified Eligible Operating Systems
: https://www.suse.com/partners/ihv/yes/yes-certified-eligible-operating-systems.html

SUSE SolidDriver Program
: http://drivers.suse.com/doc/SolidDriver/

Independent Software Vendors
: https://www.suse.com/partners/isv/

SUSE Technical Support Handbook
: https://www.suse.com/support/handbook/

FAQ Support
: https://www.suse.com/support/faq.html



Teil II. System





32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung

10

SUSE® Linux Enterprise Desktop ist für 64-Bit-Plattformen verfügbar. Das bedeutet jedoch nicht unbedingt, dass alle enthaltenen Anwendungen bereits auf 64-Bit-Plattformen portiert wurden. SUSE Linux Enterprise Desktop unterstützt die Verwendung von 32-Bit-Anwendungen in einer 64-Bit-Systemumgebung. Dieses Kapitel bietet einen kurzen Überblick darüber, wie diese Unterstützung auf SUSE Linux Enterprise Desktop-64-Bit-Plattformen implementiert ist. Es wird erläutert, wie 32-Bit-Anwendungen ausgeführt werden (Laufzeitunterstützung) und wie 32-Bit-Anwendungen kompiliert werden sollten, damit sie sowohl in 32-Bit- als auch in 64-Bit-Systemanwendungen ausgeführt werden können. Außerdem finden Sie Informationen zur Kernel-API und es wird erläutert, wie 32-Bit-Anwendungen unter einem 64-Bit-Kernel ausgeführt werden können.

SUSE Linux Enterprise Desktop für die 64-Bit-Plattformen AMD64 und Intel 64 ist so konzipiert, dass bestehende 32-Bit-Anwendungen sofort in der 64-Bit-Umgebung „ausgeführt werden können.“ Diese Unterstützung bedeutet, dass Sie weiterhin Ihre bevorzugten 32-Bit-Anwendungen verwenden können und nicht warten müssen, bis ein entsprechender 64-Bit-Port verfügbar ist.

10.1 Laufzeitunterstützung

WICHTIG: Konflikte zwischen Anwendungsversionen

Wenn eine Anwendung sowohl für 32-Bit- als auch für 64-Bit-Umgebungen verfügbar ist, führt die parallele Installation beider Versionen zwangsläufig zu Problemen. Entscheiden Sie sich in diesen Fällen für eine der beiden Versionen und installieren und verwenden Sie nur diese.

Eine Ausnahme von dieser Regel ist PAM (Pluggable Authentication Modules). Während des Authentifizierungsprozesses verwendet SUSE Linux Enterprise Desktop PAM (austauschbare Authentifizierungsmodule) als Schicht für die Vermittlung zwischen Benutzer und Anwendung. Auf einem 64-Bit-Betriebssystem, das auch 32-Bit-Anwendungen ausführt, ist es stets erforderlich, beide Versionen eines PAM-Moduls zu installieren.

Für eine korrekte Ausführung benötigt jede Anwendung eine Reihe von Bibliotheken. Leider sind die Namen für die 32-Bit- und 64-Bit-Versionen dieser Bibliotheken identisch. Sie müssen auf andere Weise voneinander unterschieden werden.

Um die Kompatibilität mit der 32-Bit-Version aufrechtzuerhalten, werden die Bibliotheken am selben Ort im System gespeichert wie in der 32-Bit-Umgebung. Die 32-Bit-Version von `libc.so.6` befindet sich sowohl in der 32-Bit- als auch in der 64-Bit-Umgebung unter `/lib/libc.so.6`.

Alle 64-Bit-Bibliotheken und Objektdateien befinden sich in Verzeichnissen mit dem Namen `lib64`. Die 64-Bit-Objektdateien, die sich normalerweise unter `/lib` und `/usr/lib` befinden, werden nun unter `/lib64` und `/usr/lib64` gespeichert. Unter `/lib` und `/usr/lib` ist also Platz für die 32-Bit-Bibliotheken, sodass der Dateiname für beide Versionen unverändert bleiben kann.

Unterverzeichnisse von 32-Bit-Verzeichnissen namens `/lib`, deren Dateninhalt nicht von der Wortgröße abhängt, werden nicht verschoben. Das Schema entspricht LSB (Linux Standards Base) und FHS (File System Hierarchy Standard).

10.2 Software-Entwicklung

Eine Doppelarchitektur-Entwicklungswerkzeugkette (Biarch Development Toolchain) ermöglicht die Erstellung von 32-Bit- und 64-Bit-Objekten. Standardmäßig werden 64-Bit-Objekte kompiliert. 32-Bit-Objekte können durch Verwendung spezieller Flaggen erstellt werden. Bei GCC lautet diese Flagge `-m32`.

Alle Header-Dateien müssen in architekturunabhängiger Form geschrieben werden. Die installierten 32-Bit- und 64-Bit-Bibliotheken müssen eine API (Anwendungsprogrammschnittstelle) aufweisen, die zu den installierten Header-Dateien passt. Die normale SUSE Linux Enterprise Desktop-Umgebung ist gemäß diesem Prinzip konzipiert. Bei manuell aktualisierten Bibliotheken müssen Sie diese Probleme selbst lösen.

10.3 Software-Kompilierung auf Doppelarchitektur-Plattformen

Um bei einer Doppelarchitektur Binärdateien für die jeweils andere Architektur zu entwickeln, müssen die entsprechenden Bibliotheken für die zweite Architektur zusätzlich installiert werden. Diese Pakete heißen `rpmname-32bit`. Außerdem benötigen Sie die entsprechenden Header und Bibliotheken aus den `rpmname-devel`-Paketen und die Entwicklungsbibliotheken für die zweite Architektur aus `rpmname-devel-32bit`.

Die meisten Open Source-Programme verwenden eine `autoconf`-basierte Programmkonfiguration. Um mit `autoconf` ein Programm für die zweite Architektur zu konfigurieren, überschreiben Sie die normalen Compiler- und Linker-Einstellungen von `autoconf`, indem Sie das Skript `configure` mit zusätzlichen Umgebungsvariablen ausführen.

Das folgende Beispiel bezieht sich auf ein x86_64-System mit x86 als zweiter Architektur.

1 Verwenden Sie den 32-Bit-Compiler:

```
CC="gcc -m32"
```

2. Weisen Sie den Linker an, 32-Bit-Objekte zu verarbeiten (verwenden Sie stets `gcc` als Linker-Frontend):

   ```
   LD="gcc -m32"
   ```

3. Legen Sie den Assembler für die Erstellung von 32-Bit-Objekten fest:

   ```
   AS="gcc -c -m32"
   ```

4. Geben Sie die Linker-Flags an, wie zum Beispiel den Standort von 32-Bit-Bibliotheken:

   ```
   LDFLAGS="-L/usr/lib"
   ```

5. Geben Sie den Standort für die 32-Bit-Objektcode-Bibliotheken an:

   ```
   --libdir=/usr/lib
   ```

6. Geben Sie den Standort für die 32-Bit-X-Bibliotheken an:

   ```
   --x-libraries=/usr/lib
   ```

Nicht alle diese Variablen werden für jedes Programm benötigt. Passen Sie sie an das entsprechende Programm an.

```
CC="gcc -m32"
LDFLAGS="-L/usr/lib;"
./configure --prefix=/usr --libdir=/usr/lib --x-libraries=/usr/lib
make
make install
```

10.4 Kernel-Spezifikationen

Die 64-Bit-Kernels für x86_64 bieten sowohl eine 64-Bit- als auch eine 32-Bit-Kernel-ABI (binäre Anwendungsschnittstelle). Letztere ist mit der ABI für den entsprechenden 32-Bit-Kernel identisch. Das bedeutet, dass die 32-Bit-Anwendung mit dem 64-Bit-Kernel auf die gleiche Weise kommunizieren kann wie mit dem 32-Bit-Kernel.

Die 32-Bit-Emulation der Systemaufrufe für einen 64-Bit-Kernel unterstützt nicht alle APIs, die von Systemprogrammen verwendet werden. Dies hängt von der Plattform ab. Aus diesem Grund muss eine kleine Zahl von Anwendungen, wie beispielsweise `lspci`, kompiliert werden.

Ein 64-Bit-Kernel kann nur 64-Bit-Kernel-Module laden, die speziell für diesen Kernel kompiliert wurden. 32-Bit-Kernel-Module können nicht verwendet werden.

TIPP: Kernel-ladbare Module

Für einige Anwendungen sind separate, Kernel-ladbare Module erforderlich. Wenn Sie vorhaben, eine solche 32-Bit-Anwendung in einer 64-Bit-Systemumgebung zu verwenden, wenden Sie sich an den Anbieter dieser Anwendung und an SUSE, um sicherzustellen, dass die 64-Bit-Version des Kernel-ladbaren Moduls und die kompilierte 32-Bit-Version der Kernel-API für dieses Modul verfügbar sind.



Booten und Konfigurieren eines Linux-Systems 11

Das Booten eines Linux-Systems umfasst verschiedene Komponenten. Die Hardware selbst wird vom BIOS initialisiert, das den Kernel mithilfe eines Bootloaders startet. Jetzt wird der Bootvorgang mit `init` und den Runlevels vollständig vom Betriebssystem gesteuert. Mithilfe des Runlevel-Konzepts können Sie Setups für die tägliche Verwendung einrichten und Wartungsaufgaben am System ausführen.

11.1 Der Linux-Bootvorgang

Der Linux-Bootvorgang besteht aus mehreren Phasen, von denen jede einer anderen Komponente entspricht. In der folgenden Liste werden der Bootvorgang und die daran beteiligten Komponenten kurz zusammengefasst.

1. **BIOS** Nach dem Einschalten des Computers initialisiert das BIOS den Bildschirm und die Tastatur und testet den Hauptspeicher. Bis zu dieser Phase greift der Computer nicht auf Massenspeichergeräte zu. Anschließend werden Informationen zum aktuellen Datum, zur aktuellen Uhrzeit und zu den wichtigsten Peripheriegeräten aus den CMOS-Werten geladen. Wenn die erste Festplatte und deren Geometrie erkannt wurden, geht die Systemkontrolle vom BIOS an den Bootloader über.

2. **Bootloader** Der erste physische 512 Byte große Datensektor der ersten Festplatte wird in den Arbeitsspeicher geladen und der *Bootloader*, der sich am Anfang dieses Sektors befindet, übernimmt die Steuerung. Die vom Bootloader ausgegebenen Befehle bestimmen den verbleibenden Teil des Bootvorgangs. Aus diesem Grund werden die ersten 512 Byte auf der ersten Festplatte als *Master Boot Record* (MBR) bezeichnet. Der Bootloader übergibt die Steuerung anschließend an das eigentliche

Betriebssystem, in diesem Fall an den Linux-Kernel. Weitere Informationen zu GRUB, dem Linux-Bootloader, finden Sie unter Kapitel 12, *Der Bootloader GRUB* (S. 151).

3. **Kernel und `initramfs`** Um die Systemsteuerung zu übergeben, lädt der Bootloader sowohl den Kernel als auch ein initiales RAM-basiertes Dateisystem (`initramfs`) in den Arbeitsspeicher. Die Inhalte der Datei `initramfs` können direkt vom Kernel verwendet werden. `initramfs` enthält eine kleine ausführbare Datei namens `init`, die das Einhängen des Root-Dateisystems übernimmt. Spezielle Hardware-Treiber für den Zugriff auf den Massenspeicher müssen in `initramfs` vorhanden sein. Weitere Informationen zu `initramfs` finden Sie unter Abschnitt 11.1.1, „`initramfs`" (S. 132).

4. **`init` unter `initramfs`** Dieses Programm führt alle für das Einhängen des entsprechenden Root-Dateisystems erforderlichen Aktionen aus, z. B. das Bereitstellen der Kernel-Funktionalität für die erforderlichen Dateisystem- und Gerätetreiber der Massenspeicher-Controller mit `udev`. Nachdem das Root-Dateisystem gefunden wurde, wird es auf Fehler geprüft und eingehängt. Wenn dieser Vorgang erfolgreich ist, wird das `initramfs` bereinigt und das `init`-Programm wird für das Root-Dateisystem ausgeführt. Weitere Informationen zum `init`-Programm finden Sie in Abschnitt 11.1.2, „init unter `initramfs`" (S. 134). Weitere Informationen zu `udev` finden Sie in Kapitel 16, *Gerätemanagement über dynamischen Kernel mithilfe von `udev`* (S. 225).

5. **`init`** Das `init`-Programm führt den eigentlichen Boot-Vorgang des Systems über mehrere unterschiedliche Ebenen aus und stellt dabei die unterschiedlichen Funktionalitäten zur Verfügung. Eine Beschreibung des `init`-Programms finden Sie in Abschnitt 11.2, „Der `init`-Vorgang" (S. 135).

11.1.1 `initramfs`

`initramfs` ist ein kleines cpio-Archiv, das der Kernel auf einen RAM-Datenträger laden kann. Es stellt eine minimale Linux-Umgebung bereit, die das Ausführen von Programmen ermöglicht, bevor das eigentliche Root-Dateisystem eingehängt wird. Diese minimale Linux-Umgebung wird von BIOS-Routinen in den Arbeitsspeicher geladen und hat, abgesehen von ausreichend Arbeitsspeicher, keine spezifischen Hardware-Anforderungen. `initramfs` muss immer eine Programmdatei namens

init zur Verfügung stellen, die das eigentliche init-Programm für das Root-Dateisystem ausführt, damit der Boot-Vorgang fortgesetzt werden kann.

Bevor das Root-Dateisystem eingehängt und das Betriebssystem gestartet werden kann, ist es für den Kernel erforderlich, dass die entsprechenden Treiber auf das Gerät zugreifen, auf dem sich das Root-Dateisystem befindet. Diese Treiber können spezielle Treiber für bestimmte Arten von Festplatten oder sogar Netzwerktreiber für den Zugriff auf ein Netzwerk-Dateisystem umfassen. Die erforderlichen Module für das Root-Dateisystem können mithilfe von init oder initramfs geladen werden. Nachdem die Module geladen wurden, stellt udev das initramfs mit den erforderlichen Geräten bereit. Später im Boot-Vorgang, nach dem Ändern des Root-Dateisystems, müssen die Geräte regeneriert werden. Dies erfolgt durch boot.udev mit dem Kommando udevtrigger.

Wenn in einem installierten System Hardwarekomponenten (z. B. Festplatten) ausgetauscht werden müssen und diese Hardware zur Boot-Zeit andere Treiber im Kernel erfordert, müssen Sie das initramfs aktualisieren. Sie gehen hierbei genauso vor wie bei der Aktualisierung des Vorgängers init: Rufen Sie mkinitrd auf. Durch das Aufrufen von mkinitrd ohne Argumente wird ein initramfs erstellt. Durch das Aufrufen von mkinitrd -R wird ein init erstellt. In SUSE® Linux Enterprise Desktop werden die zu ladenden Module durch die Variable INITRD_MODULES in /etc/sysconfig/kernel angegeben. Nach der Installation wird diese Variable automatisch auf den korrekten Wert eingestellt. Die Module werden genau in der Reihenfolge geladen, in der sie in INITRD_MODULES angezeigt werden. Dies ist nur wichtig, wenn Sie sich auf die korrekte Einstellung der Gerätedateien /dev/sd? verlassen. In bestehenden Systemen können Sie jedoch auch die Gerätedateien unter /dev/disk/ verwenden, die in mehreren Unterverzeichnissen angeordnet sind (by-id, by-path und by-uuid) und stets dieselbe Festplatte darstellen. Dies ist auch während der Installation durch Angabe der entsprechenden Einhängeoption möglich.

WICHTIG: Aktualisieren von initramfs oder init

Der Bootloader lädt initramfs oder init auf dieselbe Weise wie den Kernel. Es ist nicht erforderlich, GRUB nach der Aktualisierung von initramfs oder init neu zu installieren, da GRUB beim Booten das Verzeichnis nach der richtigen Datei durchsucht.

11.1.2 init unter `initramfs`

Der Hauptzweck von `init` unter `initramfs` ist es, das Einhängen des eigentlichen Root-Dateisystems sowie die Vorbereitung des Zugriffs darauf. Je nach aktueller Systemkonfiguration ist `init` für die folgenden Tasks verantwortlich.

Laden der Kernelmodule
: Je nach Hardwarekonfiguration sind für den Zugriff auf die Hardwarekomponenten des Computers (vor allem auf die Festplatte) spezielle Treiber erforderlich. Für den Zugriff auf das eigentliche Root-Dateisystem muss der Kernel die entsprechenden Dateisystemtreiber laden.

Bereitstellen von speziellen Blockdateien
: Der Kernel generiert Geräteereignisse für alle geladenen Module. `udev` verarbeitet diese Ereignisse und generiert die erforderlichen blockspezifischen Dateien auf einem RAM-Dateisystem im Verzeichnis `/dev`. Ohne diese speziellen Dateien wäre ein Zugriff auf das Dateisystem und andere Geräte nicht möglich.

Verwalten von RAID- und LVM-Setups
: Wenn Ihr System so konfiguriert ist, dass das Root-Dateisystem sich unter RAID oder LVM befindet, richtet `init` LVM oder RAID so ein, dass der Zugriff auf das Root-Dateisystem zu einem späteren Zeitpunkt erfolgt. Informationen über RAID und LVM finden Sie in Kapitel 12, *Fortgeschrittene Festplattenkonfiguration* (↑*Bereitstellungshandbuch*).

Verwalten von Netzwerkkonfigurationen
: Wenn Ihr System für die Verwendung eines Netzwerk-eingehängten Root-Dateisystems (über NFS eingehängt) konfiguriert ist, muss `init` sicherstellen, dass die entsprechenden Netzwerktreiber geladen und für den Zugriff auf das Root-Dateisystem eingerichtet werden.

Wenn `init` im Rahmen des Installationsvorgangs während des anfänglichen Boot-Vorgangs aufgerufen wird, unterscheiden sich seine Tasks von den oben beschriebenen:

Suchen des Installationsmediums
: Wenn Sie den Installationsvorgang starten, lädt Ihr Computer vom Installationsmedium einen Installationskernel und ein spezielles `init` mit dem YaST-Installationsprogramm. Das YaST-Installationsprogramm, das in einem RAM-Dateisystem

ausgeführt wird, benötigt Daten über den Speicherort des Installationsmediums, um auf dieses zugreifen und das Betriebssystem installieren zu können.

Initiieren der Hardware-Erkennung und Laden der entsprechenden Kernelmodule
: Wie unter Abschnitt 11.1.1, „`initramfs`“ (S. 132) beschrieben, startet der Boot-Vorgang mit einem Mindestsatz an Treibern, die für die meisten Hardwarekonfigurationen verwendet werden können. `init` startet einen anfänglichen Hardware-Scan-Vorgang, bei dem die für die Hardwarekonfiguration geeigneten Treiber ermittelt werden. Die für den Boot-Vorgang benötigten Namen der Module werden in `INITRD_MODULES` in das Verzeichnis `/etc/sysconfig/kernel` geschrieben. Diese Namen werden verwendet, um ein benutzerdefiniertes `initramfs` zu erstellen, das zum Booten des Systems benötigt wird. Wenn die Module nicht zum Booten, sondern für coldplug benötigt werden, werden die Module in `/etc/sysconfig/hardware/hwconfig-*` geschrieben. Alle Geräte, die durch Konfigurationsdateien in diesem Verzeichnis beschrieben werden, werden beim Boot-Vorgang initialisiert.

Laden des Installations- oder Rettungssystems
: Sobald die Hardware korrekt erkannt wurde, werden die entsprechenden Treiber geladen und `udev` erstellt die entsprechenden Gerätedateien, `init` startet das Installationssystem mit dem YaST-Installationsprogramm bzw. das Rettungssystem.

Starten von YaST
: `init` startet schließlich YaST, das wiederum die Paketinstallation und die Systemkonfiguration startet.

11.2 Der `init`-Vorgang

Das Programm `init` ist der Prozess mit der ID 1. Er ist verantwortlich für die erforderliche Initialisierung des Systems. `init` wird direkt durch den Kernel gestartet und ist nicht anfällig für „Signal 9“, das Prozesse normalerweise beendet. Alle anderen Programme werden entweder direkt von `init` oder von einem seiner untergeordneten Prozesse gestartet.

init wird zentral in der Datei `/etc/inittab` konfiguriert, in der auch die *Runlevel* definiert werden (siehe Abschnitt 11.2.1, „Runlevel“ (S. 136)). Diese Datei legt auch fest, welche Dienste und Dämons in den einzelnen Runlevels verfügbar sind. Je nach

den Einträgen in /etc/inittab werden von init mehrere Skripten ausgeführt. Standardmäßig wird nach dem Booten als erstes Skript /etc/init.d/boot gestartet. Nach Abschluss der Systeminitialisierung ändert das System den Runlevel mithilfe des Skripts /etc/init.d/rc auf seinen Standard-Runlevel. Diese Skripten, die der Deutlichkeit halber als *init-Skripten* bezeichnet werden, befinden sich im Verzeichnis /etc/init.d (siehe Abschnitt 11.2.2, „Init-Skripten“ (S. 139)).

Der gesamte Vorgang des Startens und Herunterfahrens des Systems wird von init verwaltet. Vor diesem Hintergrund kann der Kernel als Hintergrundprozess betrachtet werden, der alle anderen Prozesse verwaltet und die CPU-Zeit sowie den Hardwarezugriff entsprechend den Anforderungen anderer Programme anpasst.

11.2.1 Runlevel

Unter Linux definieren *Runlevel*, wie das System gestartet wird und welche Dienste im laufenden System verfügbar sind. Nach dem Booten startet das System wie in /etc/inittab in der Zeile initdefault definiert. Dies ist in der Regel die Einstellung 3 oder 5. Weitere Informationen hierzu finden Sie unter Tabelle 11.1, „Verfügbare Runlevel“ (S. 136). Alternativ kann der Runlevel auch zur Boot-Zeit (beispielsweise durch Einfügen der Runlevel-Nummer an der Eingabeaufforderung) angegeben werden. Alle Parameter, die nicht direkt vom Kernel ausgewertet werden können, werden an init übergeben. Zum Booten in Runlevel 3 fügen Sie der Boot-Eingabeaufforderung einfach die Ziffer 3 hinzu.

Tabelle 11.1 *Verfügbare Runlevel*

Runlevel	Beschreibung
0	Systemstopp
S or 1	Einzelbenutzer-Modus
2	Lokaler Mehrbenutzer-Modus mit entferntem Netzwerk (NFS usw.)
3	Mehrbenutzer-Vollmodus mit Netzwerk

Runlevel	Beschreibung
4	*Benutzerdefiniert*. Diese Option wird nicht verwendet, es sei denn, der Administrator konfiguriert diesen Runlevel.
5	Mehrbenutzer-Vollmodus mit Netzwerk und X-Display-Manager - KDM, GDM oder XDM
6	Systemneustart

WICHTIG: Runlevel 2 mit einer über NFS eingehängten Partition ist zu vermeiden

Sie sollten Runlevel 2 nicht verwenden, wenn Ihr System eine Partition, wie `/usr`, über NFS einhängt. Das System zeigt möglicherweise unerwartetes Verhalten, wenn Programmdateien oder Bibliotheken fehlen, da der NFS-Dienst in Runlevel 2 nicht zur Verfügung steht (lokaler Mehrbenutzer-Modus ohne entferntes Netzwerk).

Um die Runlevel während des laufenden Systembetriebs zu ändern, geben Sie `telinit` und die entsprechende Zahl als Argument ein. Dies darf nur von Systemadministratoren ausgeführt werden. In der folgenden Liste sind die wichtigsten Befehle im Runlevel-Bereich aufgeführt.

`telinit 1` oder `shutdown now`
: Das System wechselt in den *Einzelbenutzer-Modus*. Dieser Modus wird für die Systemwartung und administrative Aufgaben verwendet.

`telinit 3`
: Alle wichtigen Programme und Dienste (einschließlich Netzwerkprogramme und -dienste) werden gestartet und reguläre Benutzer können sich anmelden und mit dem System ohne grafische Umgebung arbeiten.

`telinit 5`
: Die grafische Umgebung wird aktiviert. Normalerweise wird ein Display-Manager, wie XDM, GDM oder KDM, gestartet. Wenn Autologin aktiviert ist, wird der

lokale Benutzer beim vorausgewählten Fenster-Manager (GNOME, KDE oder einem anderem Fenster-Manager) angemeldet.

`telinit 0` oder `shutdown -h now`
: Das System wird gestoppt.

`telinit 6` oder `shutdown -r now`
: Das System wird gestoppt und anschließend neu gestartet.

Runlevel `5` ist der standardmäßige Runlevel bei allen Standardinstallationen von SUSE Linux Enterprise Desktop. Die Benutzer werden aufgefordert, sich mit einer grafischen Oberfläche anzumelden, oder der Standardbenutzer wird automatisch angemeldet.

WARNUNG: Fehler in `/etc/inittab` können zu einem fehlerhaften Systemstart führen

Wenn `/etc/inittab` beschädigt ist, kann das System möglicherweise nicht ordnungsgemäß gebootet werden. Daher müssen Sie bei der Bearbeitung von `/etc/inittab` extrem vorsichtig sein. Lassen Sie `init` stets `/etc/inittab` mit dem Kommando `telinit q` neu lesen, bevor Sie den Computer neu starten.

Beim Ändern der Runlevel geschehen in der Regel zwei Dinge. Zunächst werden Stopp-Skripten des aktuellen Runlevel gestartet, die einige der für den aktuellen Runlevel wichtigen Programme schließen. Anschließend werden die Start-Skripten des neuen Runlevel gestartet. Dabei werden in den meisten Fällen mehrere Programme gestartet. Beim Wechsel von Runlevel 3 zu 5 wird beispielsweise Folgendes ausgeführt:

1. Der Administrator (`root`) fordert init durch die Eingabe des Befehls `telinit 5` auf, zu einem anderen Runlevel zu wechseln.

2. init prüft den aktuellen Runlevel (`Runlevel`) und stellt fest, dass `/etc/init.d/rc` mit dem neuen Runlevel als Parameter gestartet werden soll.

3. Jetzt ruft `rc` die Stopp-Skripten des aktuellen Runlevel auf, für die es im neuen Runlevel keine Start-Skripten gibt. In diesem Beispiel sind dies alle Skripten, die sich in `/etc/init.d/rc3.d` (alter Runlevel war 3) befinden und mit einem `K` beginnen. Die Zahl nach `K` gibt die Reihenfolge an, in der die Skripten mit dem

Parameter `stop` ausgeführt werden sollen, da einige Abhängigkeiten berücksichtigt werden müssen.

4. Die Start-Skripten des neuen Runlevel werden zuletzt gestartet. In diesem Beispiel befinden sie sich im Verzeichnis `/etc/init.d/rc5.d` und beginnen mit einem `S`. Auch hier legt die nach dem `S` angegebene Zahl die Reihenfolge fest, in der die Skripten gestartet werden sollen.

Bei dem Wechsel in denselben Runlevel wie der aktuelle Runlevel prüft `init` nur `/etc/inittab` auf Änderungen und startet die entsprechenden Schritte, z. B. für das Starten von `getty` auf einer anderen Schnittstelle. Dieselbe Funktion kann durch den Befehl `telinit q` erreicht werden.

11.2.2 Init-Skripten

Im Verzeichnis `/etc/init.d` gibt es zwei Skripttypen:

Skripte, die direkt von `init` ausgeführt werden
: Dies ist nur während des Boot-Vorgangs der Fall oder wenn das sofortige Herunterfahren des Systems initiiert wird (Stromausfall oder Drücken der Tastenkombination Strg + Alt + Entf). Die Ausführung dieser Skripten ist in `/etc/inittab` definiert.

Skripte, die indirekt von `init` ausgeführt werden
: Diese werden beim Wechsel des Runlevels ausgeführt und rufen immer das Master-Skript `/etc/init.d/rc` auf, das die richtige Reihenfolge der relevanten Skripten gewährleistet.

Sämtliche Skripten befinden sich im Verzeichnis `/etc/init.d`. Skripten, die während des Bootens ausgeführt werden, werden über symbolische Links aus `/etc/init.d/boot.d` aufgerufen. Skripten zum Ändern des Runlevels werden jedoch über symbolische Links aus einem der Unterverzeichnisse (`/etc/init.d/rc0.d` bis `/etc/init.d/rc6.d`) aufgerufen. Dies dient lediglich der Übersichtlichkeit und der Vermeidung doppelter Skripten, wenn diese in unterschiedlichen Runlevels verwendet werden. Da jedes Skript sowohl als Start- als auch als Stopp-Skript ausgeführt werden kann, müssen sie die Parameter `start` und `stop` erkennen. Die Skripten erkennen außerdem die Optionen `restart`, `reload`, `force-reload` und `status`. Diese verschiedenen Optionen werden in Tabelle 11.2, „Mögliche `init`-Skript-Optio-

nen“ (S. 140) erläutert. Die von `init` direkt ausgeführten Skripte verfügen nicht über diese Links. Sie werden unabhängig vom Runlevel bei Bedarf ausgeführt.

***Tabelle 11.2** Mögliche init-Skript-Optionen*

Option	Beschreibung
`start`	Startet den Dienst.
`stop`	Stoppt den Dienst.
`restart`	Wenn der Dienst läuft, wird er gestoppt und anschließend neu gestartet. Wenn der Dienst nicht läuft, wird er gestartet.
`reload`	Die Konfiguration wird ohne Stoppen und Neustarten des Dienstes neu geladen.
`force-reload`	Die Konfiguration wird neu geladen, sofern der Dienst dies unterstützt. Anderenfalls erfolgt dieselbe Aktion wie bei dem Befehl `restart`.
`status`	Zeigt den aktuellen Status des Dienstes an.

Mithilfe von Links in den einzelnen Runlevel-spezifischen Unterverzeichnissen können Skripten mit unterschiedlichen Runleveln verknüpft werden. Bei der Installation oder Deinstallation von Paketen werden diese Links mithilfe des Programms „insserv“ hinzugefügt oder entfernt (oder mithilfe von `/usr/lib/lsb/install_initd`, ein Skript, das dieses Programm aufruft). Unter `man 8 insserv` finden Sie weitere Einzelheiten.

All diese Einstellungen können auch mithilfe des YaST-Moduls geändert werden. Wenn Sie den Status über die Kommandozeile prüfen, verwenden Sie das Werkzeug `chkconfig`, das auf der man-Seite `man 8 chkconfig` beschrieben ist.

Im Folgenden finden Sie eine kurze Einführung in die zuerst bzw. zuletzt gestarteten Boot- und Stopp-Skripten sowie eine Erläuterung des Steuerskripten.

boot

Werden ausgeführt, wenn das System direkt mit init gestartet wird. Es wird unabhängig vom gewählten Runlevel und nur einmalig ausgeführt. Dabei werden die Dateisysteme /proc und /dev/pts eingehängt und blogd (Boot Logging Daemon) wird aktiviert. Wenn das System nach einer Aktualisierung oder einer Installation das erste Mal gebootet wird, wird die anfängliche Systemkonfiguration gestartet.

Der blogd-Dämon ist ein Dienst, der von boot und rc vor allen anderen Diensten gestartet wird. Er wird beendet, sobald die von diesen Skripten (die eine Reihe von Unterskripte ausführen, beispielsweise um spezielle Blockdateien verfügbar zu machen) ausgelösten Aktionen abgeschlossen sind. blogd schreibt alle Bildschirmausgaben in die Protokolldatei /var/log/boot.msg, jedoch nur wenn /var mit Schreib-/Lesezugriff eingehängt ist. Anderenfalls puffert blogd alle Bildschirmdaten, bis /var zur Verfügung steht. Info man(-Kommando)

Das Skript boot ist zudem für das Starten aller Skripten in /etc/init.d/boot.d verantwortlich, deren Name mit S beginnt. Dort werden die Dateisysteme überprüft und bei Bedarf Loop-Devices konfiguriert. Außerdem wird die Systemzeit festgelegt. Wenn bei der automatischen Prüfung und Reparatur des Dateisystems ein Fehler auftritt, kann der Systemadministrator nach Eingabe des Root-Passworts eingreifen. Das zuletzt ausgeführte Skript ist boot.local.

boot.local

Hier können Sie zusätzliche Kommandos eingeben, die beim Booten ausgeführt werden sollen, bevor Sie zu einem Runlevel wechseln. Dieses Skript ist mit der AUTOEXEC.BAT in DOS-Systemen vergleichbar.

halt

Dieses Skript wird nur beim Wechsel in Runlevel 0 oder 6 ausgeführt. Hier wird es entweder als init oder als init ausgeführt. Ob das System heruntergefahren oder neu gebootet wird, hängt davon ab, wie halt aufgerufen wird. Falls beim Herunterfahren Sonderkommandos benötigt werden, fügen Sie diese dem Skript init hinzu.

rc

Dieses Skript ruft die entsprechenden Stopp-Skripten des aktuellen Runlevels und die Start-Skripten des neu gewählten Runlevels auf. Wie das Skript /etc/init

.d/boot wird auch dieses Skript über /etc/inittab mit dem gewünschten Runlevel als Parameter aufgerufen.

Sie können Ihre eigenen Skripten erstellen und diese problemlos in das oben beschriebene Schema integrieren. Anweisungen zum Formatieren, Benennen und Organisieren benutzerdefinierter Skripten finden Sie in den Spezifikationen von LSB und auf den man-Seiten von init, init.d, chkconfig und insserv. Weitere Informationen finden Sie zudem auf den man-Seiten zu startproc und killproc.

WARNUNG: Fehlerhafte init-Skripte können das System stoppen

Bei fehlerhaften init-Skripten kann es dazu kommen, dass der Computer hängt. Diese Skripten sollten mit großer Vorsicht bearbeitet werden und, wenn möglich, gründlich in der Mehrbenutzer-Umgebung getestet werden. Hilfreiche Informationen zu init-Skripten finden Sie in Abschnitt 11.2.1, „Runlevel" (S. 136).

Sie erstellen ein benutzerdefiniertes init-Skript für ein bestimmtes Programm oder einen Dienst, indem Sie die Datei /etc/init.d/skeleton als Schablone verwenden. Speichern Sie eine Kopie dieser Datei unter dem neuen Namen und bearbeiten Sie die relevanten Programm- und Dateinamen, Pfade und ggf. weitere Details. Sie können das Skript auch mit eigenen Ergänzungen erweitern, sodass die richtigen Aktionen vom init-Prozess ausgelöst werden.

Der Block INIT INFO oben ist ein erforderlicher Teil des Skripts und muss bearbeitet werden. Weitere Informationen hierzu finden Sie unter Beispiel 11.1, „Ein minimaler INIT INFO-Block" (S. 142).

Beispiel 11.1 *Ein minimaler INIT INFO-Block*

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

Geben Sie in der ersten Zeile des INFO-Blocks nach Provides: den Namen des Programms oder des Dienstes an, das bzw. der mit diesem Skript gesteuert werden soll. Geben Sie in den Zeilen Required-Start: und Required-Stop: alle Dienste

an, die weiter ausgeführt werden müssen, wenn der Dienst selbst gestoppt wird. Diese Informationen werden später zum Generieren der Nummerierung der Skriptnamen verwendet, die in den Runlevel-Verzeichnissen enthalten sind. Geben Sie nach `Default-Start:` und `Default-Stop:` die Runlevel an, in denen der Dienst automatisch gestartet oder gestoppt werden soll. Geben Sie für `Description:` schließlich eine kurze Beschreibung des betreffenden Dienstes ein.

Um in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) die Links auf die entsprechenden Skripten in `/etc/init.d/` zu erstellen, geben Sie den Befehl `insserv` *`neuer skriptname`* ein. Das Programm `insserv` wertet den `INIT INFO`-Header aus, um die erforderlichen Links für die Start- und Stopp-Skripts in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) zu erstellen. Das Programm sorgt zudem für die richtige Start- und Stopp-Reihenfolge für die einzelnen Runlevel, indem es die erforderlichen Nummern in die Namen dieser Links aufnimmt. Wenn Sie zum Erstellen der Links ein grafisches Werkzeug bevorzugen, verwenden Sie den von YaST zur Verfügung gestellten Runlevel-Editor wie in Abschnitt 11.2.3, „Konfigurieren von Systemdiensten (Runlevel) mit YaST“ (S. 143) beschrieben.

Wenn ein in `/etc/init.d/` bereits vorhandenes Skript in das vorhandene Runlevel-Schema integriert werden soll, erstellen Sie die Links in den Runlevel-Verzeichnissen direkt mit insserv oder indem Sie den entsprechenden Dienst im Runlevel-Editor von YaST aktivieren. Ihre Änderungen werden beim nächsten Neustart wirksam und der neue Dienst wird automatisch gestartet.

Diese Links dürfen nicht manuell festgelegt werden. Wenn der `INFO`-Block Fehler enthält, treten Probleme auf, wenn `insserv` zu einem späteren Zeitpunkt für einen anderen Dienst ausgeführt wird. Der manuell hinzugefügte Dienst wird bei der nächsten Ausführung von `insserv` für dieses Skript entfernt.

11.2.3 Konfigurieren von Systemdiensten (Runlevel) mit YaST

Nach dem Starten dieses YaST-Moduls mit *YaST* > *System* > *Systemdienste (Runlevel)* werden ein Überblick über alle verfügbaren Dienste sowie der aktuelle Status der einzelnen Dienste (deaktiviert oder aktiviert) angezeigt. Legen Sie fest, ob das Modul im *einfachen Modus* oder im *Expertenmodus* ausgeführt werden soll. Der vorgegebene *einfache Modus* sollte für die meisten Zwecke ausreichend sein. In der linken Spalte

wird der Name des Dienstes, in der mittleren Spalte sein aktueller Status und in der rechten Spalte eine kurze Beschreibung angezeigt. Der untere Teil des Fensters enthält eine ausführlichere Beschreibung des ausgewählten Dienstes. Um einen Dienst zu aktivieren, wählen Sie ihn in der Tabelle aus und klicken Sie anschließend auf *Aktivieren*. Führen Sie die gleichen Schritte aus, um einen Dienst zu deaktivieren.

Die detaillierte Steuerung der Runlevel, in denen ein Dienst gestartet oder gestoppt bzw. die Änderung des vorgegebenen Runlevel erfolgt im *Expertenmodus*. Der aktuell vorgegebene Runlevel oder „initdefault" (der Runlevel, in den das System standardmäßig bootet) wird oben angezeigt. Der standardmäßige Runlevel eines SUSE Linux Enterprise Desktop-Systems ist in der Regel Runlevel 5 (Mehrbenutzer-Vollmodus mit Netzwerk und X). Eine geeignete Alternative kann Runlevel 3 sein (Mehrbenutzer-Vollmodus mit Netzwerk).

In diesem YaST-Dialogfeld können Sie einen Runlevel (wie unter Tabelle 11.1, „Verfügbare Runlevel" (S. 136) aufgeführt) als neuen Standard wählen. Zudem können Sie mithilfe der Tabelle in diesem Fenster einzelne Dienste und Dämonen aktivieren oder deaktivieren. In dieser Tabelle sind die verfügbaren Dienste und Dämonen aufgelistet und es wird angezeigt, ob sie aktuell auf dem System aktiviert sind und wenn ja, für welche Runlevel. Nachdem Sie mit der Maus eine der Zeilen ausgewählt haben, klicken Sie auf die Kontrollkästchen, die die Runlevel (*B*, *0*, *1*, *2*, *3*, *5*, *6* und *S*) darstellen, um die Runlevel festzulegen, in denen der ausgewählte Dienst oder Daemon ausgeführt werden sollte. Runlevel 4 ist nicht definiert, um das Erstellen eines benutzerdefinierten Runlevel zu ermöglichen. Unterhalb der Tabelle wird eine kurze Beschreibung des aktuell ausgewählten Dienstes oder Daemons angezeigt.

WARNUNG: Fehlerhafte Runlevel-Einstellungen können das System beschädigen

Fehlerhafte Runlevel-Einstellungen können ein System unbrauchbar machen. Stellen Sie vor dem Anwenden der Änderungen sicher, dass Sie deren Auswirkungen kennen.

Abbildung 11.1 *Systemdienste (Runlevel)*



Legen Sie mit den Optionen *Start, Anhalten oder Aktualisieren* fest, ob ein Dienst aktiviert werden soll. *Status aktualisieren* prüft den aktuellen Status. *Mit Übernehmen oder Zurücksetzen* können Sie wählen, ob die Änderungen für das System angewendet werden sollen, oder ob die ursprünglichen Einstellungen wiederhergestellt werden sollen, die vor dem Starten des Runlevel-Editors wirksam waren. Mit *OK* speichern Sie die geänderten Einstellungen.

11.3 Systemkonfiguration über /etc/sysconfig

Die Hauptkonfiguration von SUSE Linux Enterprise Desktop wird über die Konfigurationsdateien in `/etc/sysconfig` gesteuert. Die einzelnen Dateien in `/etc/sysconfig` werden nur von den Skripten gelesen, für die sie relevant sind. Dadurch

wird gewährleistet, dass Netzwerkeinstellungen beispielsweise nur von netzwerkbezogenen Skripten analysiert werden.

Sie haben zwei Möglichkeiten, die Systemkonfiguration zu bearbeiten. Entweder verwenden Sie den YaST-Editor "sysconfig" oder Sie bearbeiten die Konfigurationsdateien manuell.

11.3.1 Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"

Der YaST-Editor "sysconfig" bietet ein benutzerfreundliches Frontend für die Systemkonfiguration. Ohne den eigentlichen Speicherort der zu ändernden Konfigurationsvariablen zu kennen, können Sie mithilfe der integrierten Suchfunktion dieses Moduls den Wert der Konfigurationsvariablen wie erforderlich ändern. YaST wendet diese Änderungen an, aktualisiert die Konfigurationen, die von den Werten in `sysconfig` abhängig sind, und startet die Dienste neu.

WARNUNG: Das Ändern von `/etc/sysconfig/*`-Dateien kann die Installation beschädigen

Sie sollten die Dateien `/etc/sysconfig`-Dateien nur bearbeiten, wenn Sie über ausreichende Sachkenntnisse verfügen. Das unsachgemäße Bearbeiten dieser Dateien kann zu schwerwiegenden Fehlern des Systems führen. Die Dateien in `/etc/sysconfig` enthalten einen kurzen Kommentar zu den einzelnen Variablen, der erklärt, welche Auswirkungen diese tatsächlich haben.

Abbildung 11.2 *Systemkonfiguration mithilfe des sysconfig-Editors*



Das YaST-Dialogfeld "sysconfig" besteht aus drei Teilen. Auf der linken Seite des Dialogfelds wird eine Baumstruktur aller konfigurierbaren Variablen angezeigt. Wenn Sie eine Variable auswählen, werden auf der rechten Seite sowohl die aktuelle Auswahl als auch die aktuelle Einstellung dieser Variable angezeigt. Unten werden in einem dritten Fenster eine kurze Beschreibung des Zwecks der Variable, mögliche Werte, der Standardwert und die Konfigurationsdatei angezeigt, aus der diese Variable stammt. In diesem Dialogfeld werden zudem Informationen dazu zur Verfügung gestellt, welche Konfigurationsskripten nach dem Ändern der Variable ausgeführt und welche neuen Dienste als Folge dieser Änderung gestartet werden. YaST fordert Sie zur Bestätigung der Änderungen auf und zeigt an, welche Skripts ausgeführt werden, wenn Sie *Beenden* wählen. Außerdem können Sie die Dienste und Skripten auswählen, die jetzt übersprungen und zu einem späteren Zeitpunkt gestartet werden sollen. YaST wendet alle Änderungen automatisch an und startet alle von den Änderungen betroffenen Dienste neu, damit die Änderungen wirksam werden.

11.3.2 Manuelles Ändern der Systemkonfiguration

Gehen Sie wie folgt vor, um die Systemkonfiguration manuell zu ändern:

1 Melden Sie sich als `root` an.

2 Wechseln Sie mit `telinit 1` in den Einzelbenutzer-Modus (Runlevel 1).

3 Nehmen Sie die erforderlichen Änderungen an den Konfigurationsdateien in einem Editor Ihrer Wahl vor.

   Wenn Sie die Konfigurationsdateien in `/etc/sysconfig` nicht mit YaST ändern, müssen leere Variablenwerte durch zwei Anführungszeichen (`KEYTABLE=""`) gekennzeichnet sein und Werte, die Leerzeichen enthalten, müssen in Anführungszeichen gesetzt werden. Werte, die nur aus einem Wort bestehen, müssen nicht in Anführungszeichen gesetzt werden.

4 Führen Sie `SuSEconfig` aus, um sicherzustellen, dass die Änderungen wirksam werden.

5 Mit einem Kommando wie `telinit` *`default_runlevel`* stellen Sie den vorherigen Runlevel des Systems wieder her. Ersetzen Sie *`default_runlevel`* durch den vorgegebenen Runlevel des Systems. Wählen Sie `5`, wenn Sie in den Mehrbenutzer-Vollmodus mit Netzwerk und X zurückkehren möchten, oder wählen Sie `3`, wenn Sie lieber im Mehrbenutzer-Vollmodus mit Netzwerk arbeiten möchten.

Dieses Verfahren ist hauptsächlich beim Ändern von systemweiten Einstellungen, z. B. der Netzwerkkonfiguration, relevant. Für kleinere Änderungen ist der Wechsel in den Einzelbenutzer-Modus nicht erforderlich. In diesem Modus können Sie jedoch sicherstellen, dass alle von den Änderungen betroffenen Programme ordnungsgemäß neu gestartet werden.

TIPP: Konfigurieren der automatisierten Systemkonfiguration

Um die automatisierte Systemkonfiguration von SuSEconfig zu deaktivieren, setzen Sie die Variable `ENABLE_SUSECONFIG` in `/etc/sysconfig/suseconfig` auf `no`. Wenn Sie den SUSE-Support für die Installation nutzen

möchten, darf SuSEconfig nicht deaktiviert werden. Es ist auch möglich, die automatisierte Konfiguration teilweise zu deaktivieren.



12 Der Bootloader GRUB

In diesem Kapitel wird die Konfiguration von GRUB (Grand Unified Bootloader), dem unter SUSE® Linux Enterprise Desktop verwendeten Bootloader, beschrieben. Zum Konfigurieren der Einstellungen steht ein spezielles YaST-Modul zur Verfügung. Wenn Sie mit dem Bootvorgang unter Linux nicht vertraut sind, lesen Sie die folgenden Abschnitte, um einige Hintergrundinformationen zu erhalten. In diesem Kapitel werden zudem einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen beschrieben.

ANMERKUNG: Kein GRUB auf Computern, die UEFI verwenden

GRUB wird routinemäßig auf Computern installiert, die mit einem traditionellen BIOS ausgestattet sind, bzw. auf UEFI (Unified Extensible Firmware Interface)-Computern, die ein kompatibles Supportmodul (Compatibility Support Module, CSM) verwenden. Auf UEFI-Computern ohne aktiviertes CSM wird automatisch `eLILO` installiert (vorausgesetzt, dass DVD1 erfolgreich gestartet wurde). Details finden Sie in der eLILO-Dokumentation unter `/usr/share/doc/packages/elilo/` auf Ihrem System.

Dieses Kapitel konzentriert sich auf das Bootmanagement und die Konfiguration des Bootloaders GRUB. Eine Übersicht über den Bootvorgang finden Sie in Kapitel 11, *Booten und Konfigurieren eines Linux-Systems* (S. 131). Ein Bootloader stellt die Schnittstelle zwischen Computer (BIOS) und dem Betriebssystem (SUSE Linux Enterprise Desktop) dar. Die Konfiguration des Bootloaders wirkt sich direkt auf das Starten des Betriebssystems aus.

In diesem Kapitel werden folgende Begriffe regelmäßig verwendet und daher ausführlicher beschrieben:

MBR (Master Boot Record)
: Die Struktur des MBR ist durch eine vom Betriebssystem unabhängige Konvention festgelegt. Die ersten 446 Byte sind für Programmcode reserviert. Sie enthalten typischerweise einen Teil eines Bootloader-Programms oder eine Betriebssystemauswahl. Die nächsten 64 Byte bieten Platz für eine Partitionstabelle mit bis zu vier Einträgen. Die Partitionstabelle enthält Informationen zur Partitionierung der Festplatte und zu Dateisystemtypen. Das Betriebssystem benötigt diese Tabelle für die Verwaltung der Festplatte. Beim konventionellen generischen Code im MBR muss genau eine Partition als *aktiv* markiert sein. Die letzten beiden Byte müssen eine statische „magische Zahl" (`AA55`) enthalten. Ein MBR, der dort einen anderen Wert enthält, wird von einigen BIOS als ungültig und daher nicht zum Booten geeignet angesehen.

Bootsektoren
: Bootsektoren sind die jeweils ersten Sektoren der Festplattenpartitionen, außer bei der erweiterten Partition, die nur ein „Container" für andere Partitionen ist. Diese Bootsektoren reservieren 512 Byte Speicherplatz für Code, der ein auf dieser Partition befindliches Betriebssystem starten kann. Dies gilt für Bootsektoren formatierter DOS-, Windows- oder OS/2-Partitionen, die zusätzlich noch wichtige Basisdaten des Dateisystems enthalten. Im Gegensatz dazu sind Bootsektoren von Linux-Partitionen nach der Einrichtung eines anderen Dateisystems als XFS zunächst leer. Eine Linux-Partition ist daher nicht durch sich selbst bootfähig, auch wenn sie einen Kernel und ein gültiges root-Dateisystem enthält. Ein Bootsektor mit gültigem Code für den Systemstart trägt in den letzten 2 Byte dieselbe „magische" Zahl wie der MBR (`AA55`).

12.1 Booten mit GRUB

GRUB umfasst zwei Stufen. Stadium 1 besteht aus 512 Byte und die einzige Aufgabe besteht drin, das zweite Stadium des Bootloaders zu laden. Anschließend wird Stufe 2 (stage2) geladen. Diese Stufe enthält den Hauptteil des Bootloaders.

In einigen Konfigurationen gibt es eine zusätzliche Zwischenstufe 1.5, die Stufe 2 von einem geeigneten Dateisystem lokalisiert und lädt. Wenn diese Methode zur Verfügung

steht, wird sie bei der Installation oder bei der anfänglichen Einrichtung von GRUB mit YaST standardmäßig gewählt.

stage2 kann auf zahlreiche Dateisysteme zugreifen. Derzeit werden ext2, ext3, ReiserFS, Minix und das von Windows verwendete DOS FAT-Dateisystem unterstützt. Bis zu einem gewissen Grad werden auch die von BSD-Systemen verwendeten , XFS, UFS und FFS unterstützt. Seit Version 0.95 kann GRUB auch von einer CD oder DVD booten, die das ISO 9660-Standarddateisystem nach der „El Torito"-Spezifikation enthält. GRUB kann noch vor dem Booten auf Dateisysteme unterstützter BIOS-Disk-Devices (vom BIOS erkannte Disketten, Festplatten, CD- oder DVD-Laufwerke) zugreifen. Daher ist keine Neuinstallation des Bootmanagers nötig, wenn die Konfigurationsdatei von GRUB (`menu.lst`) geändert wird. Beim Booten des Systems liest GRUB die Menüdatei samt der aktuellen Pfade und Partitionsdaten zur Kernel oder zur Initial RAM-Disk (`initrd`) neu ein und findet diese Dateien selbstständig.

Die eigentliche Konfiguration von GRUB basiert auf den im Folgenden beschriebenen vier Dateien:

`/boot/grub/menu.lst`
: Diese Datei enthält sämtliche Informationen zu Partitionen oder Betriebssystemen, die mit GRUB gebootet werden können. Wenn diese Angaben nicht zur Verfügung stehen, wird der Benutzer in der GRUB-Kommandozeile danach gefragt (siehe Abschnitt 12.1.1.3, „Ändern von Menü-Einträgen während des Bootvorgangs" (S. 159)).

`/boot/grub/device.map`
: Diese Datei übersetzt Gerätenamen aus der GRUB- und BIOS-Notation in Linux-Gerätenamen.

`/etc/grub.conf`
: Diese Datei enthält die Befehle, Parameter und Optionen, die die GRUB-Shell für das ordnungsgemäße Installieren des Bootloaders benötigt.

`/etc/sysconfig/bootloader`
: Diese Datei wird von der Perl Bootloader-Bibliothek gelesen, die bei der Konfiguration des Bootloaders mit YaST und bei jeder Installation eines neuen Kernels verwendet wird. Sie enthält Konfigurationsoptionen (wie Kernel-Parameter), die standardmäßig zur Bootloader-Konfigurationsdatei hinzugefügt werden.

GRUB kann auf mehrere Weisen gesteuert werden. Booteinträge aus einer vorhandenen Konfiguration können im grafischen Menü (Eröffnungsbildschirm) ausgewählt werden. Die Konfiguration wird aus der Datei `menu.lst` geladen.

In GRUB können alle Bootparameter vor dem Booten geändert werden. Auf diese Weise können beispielsweise Fehler behoben werden, die beim Bearbeiten der Menüdatei aufgetreten sind. Außerdem können über eine Art Eingabeaufforderung Bootkommandos interaktiv eingegeben werden. Weitere Informationen finden Sie in Abschnitt 12.1.1.3, „Ändern von Menü-Einträgen während des Bootvorgangs" (S. 159). GRUB bietet die Möglichkeit, noch vor dem Booten die Position des Kernels und von `initrd` festzustellen. Auf diese Weise können Sie auch ein installiertes Betriebssystem booten, für das in der Konfiguration des Bootloaders noch kein Eintrag vorhanden ist.

GRUB ist in zwei Versionen vorhanden: als Bootloader und als normales Linux-Programm in `/usr/sbin/grub`. Letzteres wird als *GRUB-Shell* bezeichnet. Es stellt auf dem installierten System eine Emulation von GRUB bereit, die zum Installieren von GRUB oder zum Testen neuer Einstellungen verwendet werden kann. Die Funktionalität, GRUB als Bootloader auf einer Festplatte oder Diskette zu installieren, ist in Form des Kommandos `setup` in GRUB integriert. Diese Befehle sind in der GRUB-Shell verfügbar, wenn Linux geladen ist.

12.1.1 Die Datei /boot/grub/menu.lst

Hinter dem grafischen Eröffnungsbildschirm mit dem Bootmenü steht die GRUB-Konfigurationsdatei `/boot/grub/menu.lst`, die alle Informationen zu allen Partitionen oder Betriebssystemen enthält, die über das Menü gebootet werden können.

GRUB liest bei jedem Systemstart die Menüdatei vom Dateisystem neu ein. Es besteht also kein Bedarf, GRUB nach jeder Änderung an der Datei neu zu installieren. Mit dem YaST-Bootloader können Sie die GRUB-Konfiguration wie in Abschnitt 12.2, „Konfigurieren des Bootloaders mit YaST" (S. 164) beschrieben ändern.

Die Menüdatei enthält Befehle. Die Syntax ist sehr einfach. Jede Zeile enthält einen Befehl, gefolgt von optionalen Parametern, die wie bei der Shell durch Leerzeichen getrennt werden. Einige Befehle erlauben aus historischen Gründen ein Gleichheitszeichen (=) vor dem ersten Parameter. Kommentare werden durch ein Rautezeichen (#) eingeleitet.

Zur Erkennung der Menüeinträge in der Menü-Übersicht, müssen Sie für jeden Eintrag einen Namen oder einen `title` vergeben. Der nach dem Schlüsselwort `title` stehende Text wird inklusive Leerzeichen im Menü als auswählbare Option angezeigt. Alle Befehle bis zum nächsten `title` werden nach Auswahl dieses Menüeintrags ausgeführt.

Der einfachste Fall ist die Umleitung zu Bootloadern anderer Betriebssysteme. Der Befehl lautet `chainloader` und das Argument ist normalerweise der Bootblock einer anderen Partition in der Blocknotation von GRUB. Beispiel:

```
chainloader (hd0,3)+1
```

Die Gerätenamen in GRUB werden in Abschnitt 12.1.1.1, „Namenskonventionen für Festplatten und Partitionen" (S. 156) beschrieben. Dieses Beispiel spezifiziert den ersten Block der vierten Partition auf der ersten Festplatte.

Mit dem Befehl `kernel` wird ein Kernel-Image angegeben. Das erste Argument ist der Pfad zum Kernel-Image auf einer Partition. Die restlichen Argumente werden dem Kernel in seiner Kommandozeile übergeben.

Wenn der Kernel nicht über die erforderlichen Treiber für den Zugriff auf die Root-Partition verfügt oder ein neueres Linux-System mit erweiterten Hotplug-Funktionen verwendet wird, muss `initrd` mit einem separaten GRUB-Befehl angegeben werden, dessen einziges Argument der Pfad zu der Datei `initrd` ist. Da die Ladeadresse von `initrd` in das geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` auf den Befehl `kernel` folgen.

Der Befehl `root` vereinfacht die Angabe der Kernel- und initrd-Dateien. Das einzige Argument von `root` ist ein Gerät oder eine Partition. Allen Kernel-, `initrd`- oder anderen Dateipfaden, für die nicht explizit ein Gerät angegeben ist, wird bis zum nächsten `root`-Befehl das Gerät vorangestellt.

Am Ende jeden Menüeintrags steht implizit der `boot`-Befehl, sodass dieser nicht in die Menüdatei geschrieben werden muss. Wenn Sie GRUB jedoch interaktiv zum Booten verwenden, müssen Sie den `boot`-Befehl am Ende eingeben. Der Befehl selbst hat keine Argumente. Er führt lediglich das geladene Kernel-Image oder den angegebenen Chainloader aus.

Wenn Sie alle Menüeinträge geschrieben haben, müssen Sie einen Eintrag als `default` festlegen. Anderenfalls wird der erste Eintrag (Eintrag `0`) verwendet. Sie haben auch die Möglichkeit, ein Zeitlimit in Sekunden anzugeben, nach dem der default-Eintrag

gebootet wird. `timeout` und `default` werden den Menüeinträgen in der Regel vorangestellt. Eine Beispieldatei finden Sie in Abschnitt 12.1.1.2, „Beispiel einer Menüdatei“ (S. 157).

12.1.1.1 Namenskonventionen für Festplatten und Partitionen

Die von GRUB für Festplatten und Partitionen verwendete Namenskonvention unterscheidet sich von der, die für normale Linux-Geräte verwendet wird. Sie sind der einfachen Plattennummerierung, die das BIOS durchführt, sehr ähnlich und die Syntax gleicht derjenigen, die in manchen BSD-Derivaten verwendet wird. In GRUB beginnt die Nummerierung der Partitionen mit null. Daher ist (`hd0,0`) die erste Partition auf der ersten Festplatte. Auf einem gewöhnlichen Desktop-Computer, bei dem eine Festplatte als Primary Master angeschlossen ist, lautet der entsprechende Linux-Gerätename `/dev/sda1`.

Die vier möglichen primären Partitionen haben die Partitionsnummern `0` bis `3`. Ab `4` werden die logischen Partitionen hochgezählt:

```
(hd0,0)   first primary partition of the first hard disk
(hd0,1)   second primary partition
(hd0,2)   third primary partition
(hd0,3)   fourth primary partition (usually an extended partition)
(hd0,4)   first logical partition
(hd0,5)   second logical partition
```

In seiner Abhängigkeit von BIOS-Geräten unterscheidet GRUB nicht zwischen PATA- (IDE), SATA-, SCSI- und Hardware RAID-Geräten. Alle Festplatten, die vom BIOS oder anderen Controllern erkannt werden, werden der im BIOS voreingestellten Bootreihenfolge entsprechend nummeriert.

Leider ist eine eindeutige Zuordnung zwischen Linux-Gerätenamen und BIOS-Gerätenamen häufig nicht möglich. Es generiert die Zuordnung mithilfe eines Algorithmus und speichert sie in der Datei `device.map`, in der sie bei Bedarf bearbeitet werden kann. Informationen zur Datei `device.map` finden Sie in Abschnitt 12.1.2, „Die Datei „device.map““ (S. 160).

Ein vollständiger GRUB-Pfad besteht aus einem Gerätenamen, der in Klammern geschrieben wird, und dem Pfad der Datei im Dateisystem auf der angegebenen Partition. Der Pfad beginnt mit einem Schrägstrich. Auf einem System mit einer einzelnen PATA-

(IDE)-Festplatte und Linux auf der ersten Partition könnte der bootbare Kernel beispielsweise wie folgt spezifiziert werden:

```
(hd0,0)/boot/vmlinuz
```

12.1.1.2 Beispiel einer Menüdatei

Das folgende Beispiel zeigt die Struktur einer GRUB-Menüdatei. Diese Beispiel-Installation beinhaltet eine Linux-Bootpartition unter `/dev/sda5`, eine Root-Partition unter `/dev/sda7` und eine Windows-Installation unter `/dev/sda1`.

```
gfxmenu (hd0,4)/boot/message❶
color white/blue black/light-gray❷
default 0❸
timeout 8❹

title linux❺
   root (hd0,4)
   kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
   initrd /boot/initrd

title windows❻
   rootnoverify (hd0,0)
   chainloader +1

title floppy❼
   rootnoverify (hd0,0)
   chainloader (fd0)+1

title failsafe❽
   root (hd0,4)
   kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
   initrd /boot/initrd.shipped
```

Der erste Block definiert die Konfiguration des Eröffnungsbildschirms:

❶ Das Hintergrundbild `message` befindet sich im `/boot`-Verzeichnis der Partition `/dev/sda5`.

❷ Farbschema: Weiß (Vordergrund), Blau (Hintergrund), Schwarz (Auswahl) und Hellgrau (Hintergrund der Markierung). Das Farbschema wirkt sich nicht auf den Eröffnungsbildschirm, sondern nur auf das anpassbare GRUB-Menü aus, auf das Sie zugreifen können, wenn Sie den Eröffnungsbildschirm mit Esc beenden.

❸ Der erste (`0`) Menüeintrag `Titel Linux` wird standardmäßig gebootet.

❹ Nach acht Sekunden ohne Benutzereingabe bootet GRUB den Standardeintrag automatisch. Um das automatische Booten zu deaktivieren, löschen Sie die Zeile `timeout`. Wenn Sie `timeout 0` setzen, bootet GRUB den Standardeintrag sofort.

Im zweiten und größten Block sind die verschiedenen bootbaren Betriebssysteme aufgelistet. Die Abschnitte für die einzelnen Betriebssysteme werden durch `title` eingeleitet.

❺ Der erste Eintrag (`title linux`) ist für das Booten von SUSE Linux Enterprise Desktop zuständig. Der Kernel (`vmlinuz`) befindet sich in der ersten logischen Partition (die Bootpartition) der ersten Festplatte. Hier werden Kernel-Parameter, z. B. die Root-Partition und der VGA-Modus, angehängt. Die Angabe der root-Partition erfolgt nach der Linux-Namenskonvention (`/dev/sda7/`), da diese Information für den Kernel bestimmt ist und nichts mit GRUB zu tun hat. Die `initrd` befindet sich ebenfalls in der ersten logischen Partition der ersten Festplatte.

❻ Der zweite Eintrag ist für das Laden von Windows verantwortlich. Windows wird von der ersten Partition der ersten Festplatte aus gebootet (`hd0,0`). Mittels `chainloader +1` wird das Auslesen und Ausführen des ersten Sektors der angegebenen Partition gesteuert.

❼ Der nächste Eintrag dient dazu, das Booten von Diskette zu ermöglichen, ohne dass dazu die BIOS-Einstellungen geändert werden müssten.

❽ Die Bootoption `failsafe` dient dazu, Linux mit einer bestimmten Auswahl an Kernel-Parametern zu starten, die selbst auf problematischen Systemen ein Hochfahren von Linux ermöglichen.

Die Menüdatei kann jederzeit geändert werden. GRUB verwendet die geänderten Einstellungen anschließend für den nächsten Bootvorgang. Sie können diese Datei mit dem Editor Ihrer Wahl oder mit YaST permanent editieren und dauerhaft speichern. Alternativ können Sie temporäre Änderungen interaktiv über die Bearbeitungsfunktion von GRUB vornehmen. Weitere Informationen hierzu finden Sie unter Abschnitt 12.1.1.3, „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 159).

12.1.1.3 Ändern von Menü-Einträgen während des Bootvorgangs

Wählen Sie im grafischen Bootmenü das zu bootende Betriebssystem mit den Pfeiltasten aus. Wenn Sie ein Linux-System wählen, können Sie in der Booteingabeaufforderung zusätzliche Bootparameter eingeben. Um einzelne Menüeinträge direkt zu bearbeiten, drücken Sie die Esc-Taste, um den Eröffnungsbildschirm zu schließen und das textbasierte GRUB-Menü anzuzeigen, und drücken Sie anschließend die Taste E. Auf diese Weise vorgenommene Änderungen gelten nur für den aktuellen Bootvorgang und können nicht dauerhaft übernommen werden.

WICHTIG: Tastaturbelegung während des Bootvorgangs

Beim Bootvorgang ist nur die amerikanische Tastaturbelegung verfügbar. Weitere Informationen hierzu finden Sie unter Abbildung 31.3, „US-Tastaturbelegung“ (S. 467).

Durch die Möglichkeit, die Menüeinträge zu bearbeiten, kann ein defektes System, das nicht mehr gebootet werden kann, repariert werden, da die fehlerhafte Konfigurationsdatei des Bootloaders mittels der manuellen Eingabe von Parametern umgangen werden kann. Die manuelle Eingabe vom Parametern während des Bootvorgangs ist zudem hilfreich zum Testen neuer Einstellungen, ohne dass diese sich auf das native System auswirken.

Aktivieren Sie den Bearbeitungsmodus und wählen Sie mithilfe der Pfeiltasten den Menüeintrag aus, dessen Konfiguration sie ändern möchten. Um die Konfiguration zu bearbeiten, drücken Sie die Taste E erneut. Auf diese Weise korrigieren Sie falsche Partitions- oder Pfadangaben, bevor sich diese negativ auf den Bootvorgang auswirken. Drücken Sie die Eingabetaste, um den Bearbeitungsmodus zu verlassen und zum Menü zurückzukehren. Drücken Sie anschließend die Taste B, um diesen Eintrag zu booten. Im Hilfetext am unteren Rand werden weitere mögliche Aktionen angezeigt.

Um die geänderten Bootoptionen dauerhaft zu übernehmen und an den Kernel zu übergeben, öffnen Sie die Datei `menu.lst` als Benutzer `root` und hängen Sie die entsprechenden Kernel-Parameter an folgende vorhandene Zeile getrennt durch Leerzeichen an:

```
title linux
   root(hd0,0)
     kernel /vmlinuz root=/dev/sda3 additional parameter
   initrd /initrd
```

GRUB übernimmt den neuen Parameter beim nächsten Booten automatisch. Alternativ können Sie diese Änderung auch mit dem YaST-Bootloader-Modul vornehmen. Hängen Sie die neuen Parameter getrennt durch Leerzeichen an die vorhandene Zeile an.

12.1.2 Die Datei „device.map“

Die Datei `device.map` enthält Zuordnungen zwischen den GRUB- und BIOS-Gerätenamen und den Linux-Gerätenamen. In einem Mischsystem aus PATA- (IDE)- und SCSI-Festplatten muss GRUB anhand eines bestimmten Verfahrens versuchen, die Bootreihenfolge zu ermitteln, da die BIOS-Informationen zur Bootreihenfolge für GRUB unter Umständen nicht zugänglich sind. GRUB speichert das Ergebnis dieser Analyse in der Datei `/boot/grub/device.map`. Ein Beispiel für `device.map`-Dateien für ein System, bei dem in der Bootreihenfolge im BIOS zuerst PATA und dann SCSI eingestellt ist:

```
(fd0)  /dev/fd0
(hd0)  /dev/sda
(hd1)  /dev/sdb
```

Alternativ:

```
(fd0)  /dev/fd0
(hd0)  /dev/disk-by-id/DISK1 ID
(hd1)  /dev/disk-by-id/DISK2 ID
```

Da die Reihenfolge von PATA- (IDE-), SCSI- und anderen Festplatten abhängig von verschiedenen Faktoren ist und Linux die Zuordnung nicht erkennen kann, besteht die Möglichkeit, die Reihenfolge in der Datei `device.map` manuell festzulegen. Wenn beim Booten Probleme auftreten sollten, prüfen Sie, ob die Reihenfolge in dieser Datei der BIOS-Reihenfolge entspricht und ändern Sie sie notfalls temporär mithilfe der GRUB-Eingabeaufforderung. Ist das Linux-System erst gebootet, können Sie die Änderungen in der Datei `device.map` mithilfe des YaST Bootloader-Moduls oder eines Editors Ihrer Wahl dauerhaft übernehmen.

Installieren Sie nach dem manuellen Bearbeiten von `device.map` GRUB mithilfe des folgenden Befehls neu. Dieser Befehl führt dazu, dass die Datei `device.map` neu geladen wird und die in `grub.conf` aufgelisteten Befehle ausgeführt werden:

```
grub --batch < /etc/grub.conf
```

12.1.3 Die Datei „/etc/grub.conf“

Nach `menu.lst` und `device.map` ist `/etc/grub.conf` die dritte wichtige Konfigurationsdatei von GRUB. Diese Datei enthält die Befehle, Parameter und Optionen, die die GRUB-Shell für das ordnungsgemäße Installieren des Bootloaders benötigt.

```
setup --stage2=/boot/grub/stage2 --force-lba (hd0,1) (hd0,1)
   quit
```

Dieses Kommando weist GRUB an, den Bootloader automatisch auf die zweite Partition der ersten Festplatte (hd0,1) zu installieren und dabei die Boot-Images zu verwenden, die sich auf derselben Partition befinden. Der Parameter `--stage2=/boot/grub/stage2` ist erforderlich, um das Image `stage2` von einem eingehängten Dateisystem zu installieren. Einige BIOS haben eine fehlerhafte Implementierung für LBA-Unterstützung. Mit `--force-lba` können Sie diese ignorieren.

12.1.4 Die Datei /etc/sysconfig/bootloader

Diese Konfigurationsdatei wird nur bei der Konfiguration des Bootloaders mit YaST und bei jeder Installation eines neuen Kernels verwendet. Sie wird von der Perl Bootloader-Bibliothek evaluiert, die die Bootloader-Konfigurationsdatei (z. B. `/boot/grub/menu.lst` für GRUB) entsprechend bearbeitet. `/etc/sysconfig/bootloader` ist keine GRUB-spezifische Konfigurationsdatei; die Werte dieser Datei gelten für alle Bootloader, die unter SUSE Linux Enterprise Desktop installiert sind.

ANMERKUNG: Bootloader-Konfiguration nach Kernel-Aktualisierung

Bei jeder Installation eines neuen Kernels schreibt der Perl Bootloader eine neue Konfigurationsdatei (z. B. `/boot/grub/menu.lst` für GRUB). Er verwendet dazu die unter `/etc/sysconfig/bootloader` angegebenen Standardeinstellungen. Wenn Sie einen angepassten Satz von Kernel-Parametern verwenden, vergewissern Sie sich, dass die entsprechenden Standardeinstellungen in `/etc/sysconfig/bootloader` wunschgemäß angepasst wurden.

`LOADER_TYPE`
: Legt den auf dem System installierten Bootloader fest (z. B. GRUB bzw. LILO). Nicht bearbeiten – Ändern Sie den Bootloader gemäß den Anweisungen unter Prozedur 12.6, „Ändern des Bootloader-Typs“ (S. 169) mit YaST.

`DEFAULT_VGA / FAILSAFE_VGA / XEN_VGA`
: Die Bildschirmauflösung und die Farbtiefe des beim Booten verwendeten Framebuffers werden mit dem Kernel-Parameter `vga` konfiguriert. Diese Werte definieren die Auflösung und die Farbtiefe, die für den standardmäßigen Boot-Eintrag, den Failsafe und den XEN-Eintrag verwendet werden. Die folgenden Werte sind zulässig:

Tabelle 12.1 *Bildschirmauflösung- und Farbtiefe-Referenz*

	640 x 480	**800 x 600**	**1024 x 768**	**1280 x 1024**	**1600 x 1200**
8bit	0x301	0x303	0x305	0x307	0x31C
15-Bit	0x310	0x313	0x316	0x319	0x31D
16-Bit	0x311	0x314	0x317	0x31A	0x31E
24-Bit	0x312	0x315	0x318	0x31B	0x31F

`DEFAULT_APPEND / FAILSAFE_APPEND / XEN_KERNEL_APPEND`
: Kernel-Parameter (außer `vga`), die automatisch an die Standard-, Failsafe- und XEN-Boot-Einträge in der Bootloader-Konfigurationsdatei angehängt werden.

`CYCLE_DETECTION / CYCLE_NEXT_ENTRY`
: Konfigurieren Sie, ob die Boot-Zyklus-Erkennung verwendet werden soll und, falls ja, welcher alternative Eintrag von `/boot/grub/menu.lst` im Fall eines Reboot-Zyklus gebootet werden soll (z. B. `Failsafe`). Detaillierte Informationen finden Sie in der `/usr/share/doc/packages/bootcycle/README`.

12.1.5 Festlegen eines Bootpassworts

GRUB unterstützt schon vor dem Booten des Betriebssystems den Zugriff auf Dateisysteme. Dies bedeutet, dass Benutzer ohne root-Berechtigungen auf Dateien des Linux-Systems zugreifen können, auf die sie nach dem Booten keinen Zugriff haben. Um diese Zugriffe oder das Booten bestimmter Betriebssysteme zu verhindern, können Sie ein Bootpasswort festlegen.

WICHTIG: Bootpasswort und Eröffnungsbildschirm

Wenn Sie für GRUB ein Bootpasswort verwenden, wird der übliche Eröffnungsbildschirm nicht angezeigt.

Legen Sie als Benutzer `root` das Bootpasswort wie folgt fest:

1 Verschlüsseln Sie an der root-Eingabeaufforderung das Passwort mithilfe von grub-md5-crypt:

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

2 Fügen Sie die verschlüsselte Zeichenkette in den globalen Abschnitt der Datei `menu.lst` ein:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

Jetzt können GRUB-Befehle in der Boot-Eingabeaufforderung nur nach Drücken der Taste P und der Eingabe des Passworts ausgeführt werden. Benutzer können jedoch über das Bootmenü weiterhin alle Betriebssysteme booten.

3 Um zu verhindern, dass ein oder mehrere Betriebssysteme über das Bootmenü gebootet werden, fügen Sie den Eintrag `lock` zu allen Abschnitten in `menu.lst` hinzu, die ohne Eingabe eines Passworts nicht gebootet werden sollen. Beispiel:

```
title linux
   kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
   initrd (hd0,4)/initrd
   lock
```

Nach dem Neubooten des Systems und der Auswahl des Linux-Eintrags im Bootmenü erscheint zunächst folgende Fehlermeldung:

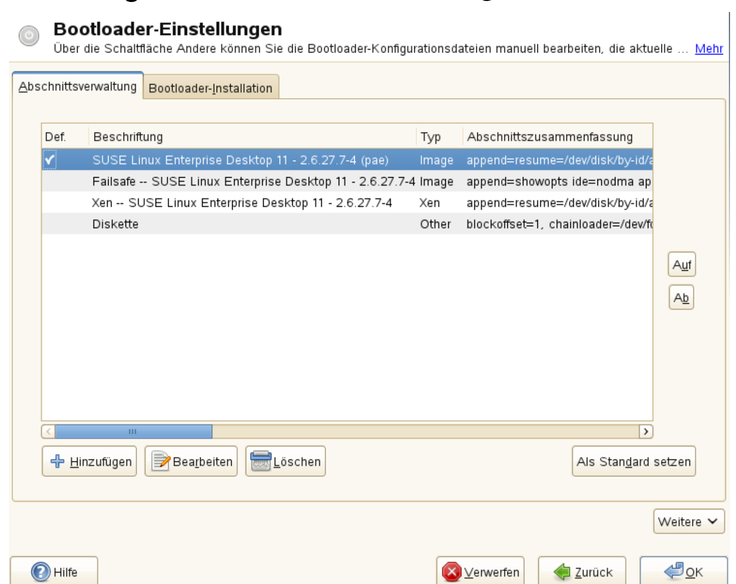
```
Error 32: Must be authenticated
```

Drücken Sie die Eingabetaste, um das Menü zu öffnen. Drücken Sie anschließend die Taste P, um die Eingabeaufforderung für das Passwort zu öffnen. Wenn Sie das Passwort eingegeben und die Eingabetaste gedrückt haben, sollte das ausgewählte Betriebssystem (in diesem Fall Linux) gebootet werden.

12.2 Konfigurieren des Bootloaders mit YaST

Mit dem YaST-Modul ist die Konfiguration des Bootloaders auf Ihrem SUSE Linux Enterprise Desktop-System am einfachsten. Wählen Sie im YaST-Kontrollzentrum die Option *System* > *Bootloader*. Wie in Abbildung 12.1, „Bootloader-Einstellungen“ (S. 164) zeigt dies die aktuelle Bootloader-Konfiguration des Systems und ermöglicht Ihnen, Änderungen vorzunehmen.

***Abbildung 12.1** Bootloader-Einstellungen*



Auf der Registerkarte *Abschnittsverwaltung* können Sie die Bootloader-Abschnitte für die einzelnen Betriebssysteme bearbeiten, ändern und löschen. Klicken Sie auf *Hinzufügen*, um eine Option hinzuzufügen. Wenn Sie den Wert einer bestehenden Option ändern möchten, wählen Sie ihn mit der Maus aus und klicken Sie auf *Bearbeiten*. Um ein vorhandenes Schema zu löschen, wählen Sie das Schema aus und klicken Sie auf *Löschen*. Wenn Sie nicht mit den Bootloader-Optionen vertraut sind, lesen Sie zunächst Abschnitt 12.1, „Booten mit GRUB" (S. 152).

Verwenden Sie die Registerkarte *Bootloader-Installation*, um die Einstellungen in Bezug auf Typ, Speicherort und erweiterte Bootloader-Einstellungen anzuzeigen und zu ändern.

Klicken Sie auf *Weitere*, um auf erweiterte Konfigurationsoptionen zuzugreifen. Über den integrierten Editor können Sie die GRUB-Konfigurationsdateien ändern. Weitere Informationen finden Sie in Abschnitt 12.1, „Booten mit GRUB" (S. 152). Sie können die vorhandene Konfiguration auch löschen und eine *neue Konfiguration ohne Vorschlag erstellen* oder sich von YaST *eine neue Konfiguration vorschlagen lassen*. Sie können die Konfiguration auch auf die Festplatte schreiben und sie von der Festplatte wieder einlesen. Zur Wiederherstellung des ursprünglichen, während der Installation gespeicherten MBR (Master Boot Record) wählen Sie *MBR von Festplatte wiederherstellen* aus.

12.2.1 Anpassen des Standard-Boot-Eintrags

Um das System zu ändern, das standardmäßig gebootet wird, gehen Sie wie folgt vor:

Prozedur 12.1 *Standardsystem einrichten*

1 Öffnen Sie die Karteireiter *Abschnittsverwaltung*.

2 Wählen Sie den gewünschten Eintrag in der Liste aus.

3 Klicken Sie auf *Als Standard festlegen*.

4 Klicken Sie auf *OK*, um die Änderungen zu aktivieren.

12.2.2 Speicherort des Bootloaders ändern

Um den Speicherort des Bootloaders zu ändern, gehen Sie wie folgt vor:

Prozedur 12.2 *Speicherort des Bootloaders ändern*

1 Wählen Sie den Karteireiter *Bootloader-Installation* und anschließend eine der folgenden Optionen für *Speicherort des Bootloaders*:

Booten vom Master Boot Record
Der Bootloader wird in den MBR des ersten Laufwerks installiert (entsprechend der im BIOS voreingestellten Bootreihenfolge).

Booten von der root-Partition
Der Bootloader wird im Bootsektor der Partition / installiert (dies ist der Standard).

Booten von der Bootpartition
Der Bootloader wird im Bootsektor der Partition `/boot` installiert.

Booten von der erweiterten Partition
Der Bootloader wird in den Container der erweiterten Partition installiert.

Benutzerdefinierte Bootpartition
Mit dieser Option können Sie den Speicherort des Bootloaders manuell angeben.

2 Klicken Sie zum Anwenden der Änderungen auf *OK*.

12.2.3 Ändern des Bootloader-Zeitlimits

Der Bootloader bootet das Standardsystem nicht sofort. Während des Zeitlimits können Sie das zu bootende System auswählen oder einige Kernel-Parameter schreiben. Gehen Sie wie folgt vor, um das Zeitlimit des Bootloaders festzulegen:

Prozedur 12.3 *Ändern des Bootloader-Zeitlimits*

1 Öffnen Sie die Karteireiter *Bootloader-Installation*.

2 Klicken Sie auf *Bootloader-Optionen*.

3. Ändern Sie den Wert für *Zeitüberschreitung in Sekunden*, indem Sie einen neuen Wert eingeben und mit der Maus auf den entsprechenden Pfeil klicken oder die Pfeiltasten der Tastatur verwenden.

4. Klicken Sie zweimal auf *OK*, um die Änderungen zu speichern.

WARNUNG: Zeitüberschreitung 0 Sekunden

Wenn Sie für die Zeitüberschreitung 0 Sekunden festlegen, können Sie während des Bootens nicht auf GRUB zugreifen. Wenn Sie als Standardbootoption gleichzeitig ein Nicht-Linux-Betriebssystem festgelegt haben, wird hierdurch der Zugriff auf das Linux-System vollständig deaktiviert.

12.2.4 Festlegen eines Bootpassworts

Mit diesem YaST-Modul können Sie zum Schutz des Bootvorgangs auch ein Passwort einrichten. Damit wird ein zusätzlicher Grad an Sicherheit geboten.

Prozedur 12.4 *Festlegen eines Bootloader-Passworts*

1. Öffnen Sie die Karteireiter *Bootloader-Installation*.

2. Klicken Sie auf *Bootloader-Optionen*.

3. Aktivieren Sie die Option *Passwort für die Menüschnittstelle* und geben Sie Ihr *Passwort* zweimal ein.

4. Klicken Sie zweimal auf *OK*, um die Änderungen zu speichern.

12.2.5 Anpassen der Festplattenreihenfolge

Wenn Ihr Computer mehrere Festplatten hat, können Sie die Bootsequenz der Festplatten so festlegen, dass sie dem BIOS-Setup des Computers entsprechen (siehe Abschnitt 12.1.2, „Die Datei „device.map““ (S. 160)). Gehen Sie hierfür wie folgt vor:

Prozedur 12.5 *Festlegen der Festplattenreihenfolge*

1. Öffnen Sie die Karteireiter *Bootloader-Installation*.

2 Klicken Sie auf *Details zur Bootloader-Installation*.

3 Ändern Sie bei mehreren aufgeführten Festplatten deren Reihenfolge mit einem Klick auf *Auf* oder *Ab*.

4 Klicken Sie zweimal auf *OK*, um die Änderungen zu speichern.

12.2.6 Konfigurieren der erweiterten Optionen

Erweiterte Boot-Optionen lassen sich über *Bootloader-Installation* > *Bootloader-Optionen* konfigurieren. Normalerweise sollte es nicht erforderlich sein, die Standardeinstellungen zu ändern.

Aktives Flag in Partitionstabelle für Bootpartition festlegen
: Aktiviert die Partition, die den Bootloader enthält. Einige ältere Betriebssysteme, z. B. Windows 98, können nur von einer aktiven Partition booten.

Generischen Bootcode in MBR schreiben
: Ersetzt den aktuellen MBR durch generischen, Betriebssystem-unabhängigen Code.

Flag für Durchführung der Fehlersuche
: Stellt GRUB in den Fehlersuchmodus um, in dem Meldungen über die Plattenaktivität angezeigt werden.

Menü beim Booten ausblenden
: Blendet das Bootmenü aus und bootet den Standardeintrag.

WARNUNG

Wenn Sie das Bootmenü ausblenden, können Sie während des Bootens nicht auf GRUB zugreifen. Wenn Sie als Standardbootoption gleichzeitig ein Nicht-Linux-Betriebssystem festgelegt haben, wird hierdurch der Zugriff auf das Linux-System vollständig deaktiviert.

Use Trusted GRUB (Trusted GRUB verwenden)
: Startet Trusted GRUB, das verbürgte Computerfunktionen unterstützt.

Datei für grafisches Menü
: Pfad zur Grafikdatei, die bei der Anzeige des Boot-Bildschirms verwendet wird.

Parameter der seriellen Verbindung
: Wenn Ihr Computer über eine serielle Konsole gesteuert wird, können Sie angeben, welcher COM-Port in welcher Geschwindigkeit verwendet werden soll. Stellen Sie auch *Terminaldefinition* auf „Seriell“ ein. Einzelheiten finden Sie unter `info grub` oder http://www.gnu.org/software/grub/manual/grub.html.

Serielle Konsole verwenden
: Wenn Ihr Computer über eine serielle Konsole gesteuert wird, aktivieren Sie diese Option und geben Sie an, welcher COM-Port in welcher Geschwindigkeit verwendet werden soll. Siehe `info grub` oder http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal.

12.2.7 Ändern des Bootloader-Typs

Legen Sie den Bootloader-Typ unter *Bootloader-Installation* fest. In SUSE Linux Enterprise Desktop wird standardmäßig der Bootloader GRUB verwendet. Gehen Sie zur Verwendung von LILO oder ELILO folgendermaßen vor:

WARNUNG: LILO wird nicht unterstützt

Die Verwendung von LILO wird nicht empfohlen, da SUSE Linux Enterprise Desktop keine Unterstützung hierfür bietet. Verwenden Sie es nur in besonderen Fällen.

Prozedur 12.6 *Ändern des Bootloader-Typs*

1 Wählen Sie die Karteireiter *Bootloader-Installation*.

2 Wählen Sie unter *Bootloader* die Option *LILO*.

3 Wählen Sie in dem sich öffnenden Dialogfeld folgende Aktionen aus:

Neue Konfiguration vorschlagen
: Lässt YaST eine neue Konfiguration erstellen.

Aktuelle Konfiguration konvertieren
: Lässt YaST die aktuelle Konfiguration konvertieren. Es ist möglich, dass beim Konvertieren der Konfiguration einige Einstellungen verloren gehen.

Neue Konfiguration ohne Vorschlag erstellen
: Erstellt eine benutzerdefinierte Konfiguration. Diese Aktion ist während der Installation von SUSE Linux Enterprise Desktop nicht verfügbar.

Auf Festplatte gespeicherte Konfiguration einlesen
: Lädt Ihre eigene Datei `/etc/lilo.conf`. Diese Aktion ist während der Installation von SUSE Linux Enterprise Desktop nicht verfügbar.

4 Klicken Sie zweimal auf *OK*, um die Änderungen zu speichern.

Während der Konvertierung wird die alte GRUB -Konfiguration gespeichert. Wenn Sie sie verwenden möchten, ändern Sie einfach den Bootloader-Typ zurück in GRUB , und wählen Sie *Vor der Konvertierung gespeicherte Konfiguration wiederherstellen*. Diese Aktion ist nur auf einem installierten System verfügbar.

ANMERKUNG: Benutzerdefinierter Bootloader

Wenn Sie einen anderen Bootloader als GRUB oder LILO verwenden möchten, wählen Sie *Keinen Bootloader installieren*. Lesen Sie die Dokumentation Ihres Bootloaders sorgfältig durch, bevor Sie diese Option auswählen.

12.3 Deinstallieren des Linux-Bootloaders

Mit YaST können Sie den Linux-Bootloader deinstallieren und den Zustand des MBR wiederherstellen, der vor der Installation von Linux vorlag. YaST erstellt während der Installation automatisch eine Sicherung der ursprünglichen MBR-Version und stellt sie bei Bedarf wieder her.

Zum Deinstallieren von GRUB starten Sie YaST und klicken Sie auf *System* > *Bootloader*, um das Bootloader-Modul zu starten. Wählen Sie *Andere* > *MBR von Festplatte wiederherstellen* aus und bestätigen Sie mit *Ja, neu schreiben*.

12.4 Erstellen von Boot-CDs

Wenn beim Booten Ihres Systems unter Verwendung eines Bootmanagers Probleme auftreten oder wenn der Bootmanager auf Ihrer Festplatte nicht installiert werden kann, ist es auch möglich, eine bootfähige CD mit allen für Linux erforderlichen Startdateien zu erstellen. Hierfür muss ein CD-Brenner in Ihrem System installiert sein.

Für die Erstellung eines bootfähigen CD-ROM mit GRUB ist lediglich eine spezielle Form von *stage2* namens `stage2_eltorito` erforderlich sowie, optional, eine benutzerdefinierte Datei `menu.lst`. Die klassischen Dateien `stage1` und `stage2` sind nicht erforderlich.

Prozedur 12.7 *Erstellen von Boot-CDs*

1 Wechseln Sie in ein Verzeichnis, in dem das ISO-Image erstellt werden soll, beispielsweise: `cd /tmp`

2 Erstellen Sie ein Unterverzeichnis für GRUB und wechseln Sie in das neu erstellte `iso`-Verzeichnis:

```
mkdir -p iso/boot/grub && cd iso
```

3 Kopieren Sie den Kernel, die Dateien `stage2_eltorito`, `initrd`, `menu.lst` und `/message` nach `iso/boot/`:

```
cp /boot/vmlinuz boot/
cp /boot/initrd boot/
cp /boot/message boot/
cp /usr/lib/grub/stage2_eltorito boot/grub
cp /boot/grub/menu.lst boot/grub
```

In bestimmten Fällen (beispielsweise beim Booten mehrerer Betriebssysteme) sollten Sie auch `/boot/grub/device.map` in `boot/grub` kopieren.

4 Ersetzen Sie die Einträge `root (hdx, y)` durch `root (cd)`, sodass sie auf das CD-ROM-Gerät verweisen. Sie müssen unter Umständen auch die Pfade zur Meldungsdatei, zum Kernel und zur initrd-Datei anpassen, so dass sie auf `/boot/message`, `/boot/vmlinuz` bzw. `/boot/initrd` verweisen. Nachdem Sie die Anpassungen durchgeführt haben, sollte `menu.lst` wie im folgenden Beispiel aussehen:

```
timeout 8
default 0
gfxmenu (cd)/boot/message

title Linux
   root (cd)
   kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
   splash=verbose showopts
   initrd /boot/initrd
```

Verwenden Sie `splash=silent` anstelle von `splash=verbose`, um zu vermeiden, dass beim Bootvorgang Bootmeldungen angezeigt werden.

5 Erstellen Sie das ISO-Image mit dem folgenden Befehl:

```
genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 \
-o grub.iso /tmp/iso
```

6 Schreiben Sie die so erstellte Datei namens `grub.iso` unter Verwendung Ihres bevorzugten Dienstprogramms auf eine CD. Brennen Sie das ISO-Image nicht als Datendatei, sondern verwenden Sie die Option zum Brennen eines CD-Images, die in Ihrem Dienstprogramm angeboten wird.

12.5 Der grafische SUSE-Bildschirm

Der grafische SUSE-Bildschirm wird auf der ersten Konsole angezeigt, wenn die Option `vga=`*`Wert`* als Kernel-Parameter verwendet wird. Bei der Installation mit YaST wird diese Option automatisch in Abhängigkeit von der gewählten Auflösung und der verwendeten Grafikkarte aktiviert. Sie haben bei Bedarf drei Möglichkeiten, den SUSE-Bildschirm zu deaktivieren:

Den SUSE-Bildschirm bei Bedarf deaktivieren
: Geben Sie den Befehl `echo 0 >/proc/splash` in der Kommandozeile ein, um den grafischen Bildschirm zu deaktivieren. Um ihn wieder zu aktivieren, geben Sie den Befehl `echo 1 >/proc/splash` ein.

Den SUSE-Bildschirm standardmäßig deaktivieren
: Fügen Sie der Bootloader-Konfiguration den Kernel-Parameter `splash=0` hinzu. Weitere Informationen hierzu finden Sie in Kapitel 12, *Der Bootloader*

GRUB (S. 151). Wenn Sie jedoch den Textmodus (Standardeinstellung in früheren Versionen) bevorzugen, legen Sie Folgendes fest: `vga=normal`.

Den SUSE-Bildschirm vollständig deaktivieren
: Kompilieren Sie einen neuen Kernel und deaktivieren Sie die Option zum *Verwenden des Eröffnungsbildschirms anstelle des Bootlogos im Menü Framebuffer-Unterstützung*. Wenn Sie im Kernel die Framebuffer-Unterstützung deaktiviert haben, ist der Eröffnungsbildschirm automatisch auch deaktiviert.

WARNUNG: Keine Unterstützung

Wenn Sie einen eigenen Kernel kompilieren, kann SUSE dafür keinen Support garantieren.

12.6 Fehlersuche

In diesem Abschnitt werden einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen behandelt. Einige der Probleme werden in den Artikeln in der Support-Datenbank unter `http://www.suse.com/support` beschrieben. Verwenden Sie das Dialogfeld „Suche", um nach Schlüsselwörtern wie *GRUB*, *boot* und *Bootloader* zu suchen.

GRUB und XFS
: XFS lässt im Partitions-Bootblock keinen Platz für `stage1`. Sie dürfen also als Speicherort des Bootloaders keinesfalls eine XFS-Partition angeben. Um dieses Problem zu beheben, erstellen Sie eine separate Bootpartition, die nicht mit XFS formatiert ist.

GRUB meldet GRUB Geom Error
: GRUB überprüft die Geometrie der angeschlossenen Festplatten beim Booten des Systems. In seltenen Fällen macht das BIOS hier inkonsistente Angaben, sodass GRUB einen "GRUB Geom Error" meldet. Aktualisieren Sie in diesem Fall das BIOS.

GRUB gibt diese Fehlermeldung auch in solchen Fällen aus, wenn Linux auf einer zusätzlichen Festplatte im System installiert wurde, diese aber nicht im BIOS registriert wurde. Der erste Teil des Bootloaders*stage1* wird korrekt gefunden und

geladen, aber die zweite Stufe *stage2* wird nicht gefunden. Dieses Problem können Sie umgehen, indem Sie die neue Festplatte unverzüglich im BIOS registrieren.

System mit mehreren Festplatten startet nicht
: Möglicherweise wurde die Bootsequenz der Festplatten während der Installation von YaST falsch ermittelt. So erkennt GRUB die PATA (IDE)-Festplatte unter Umständen als `hd0` und die SCSI-Festplatte als `hd1`, obwohl im BIOS die umgekehrte Reihenfolge (SCSI *vor* PATA) angegeben ist.

  Korrigieren Sie in solchen Fällen mithilfe der GRUB-Kommandozeile beim Booten die verwendeten Festplatten. Bearbeiten Sie im gebooteten System die Datei `device.map`, um die neue Zuordnung dauerhaft festzulegen. Anschließend überprüfen Sie die GRUB-Gerätenamen in den Dateien `/boot/grub/menu.lst` und `/boot/grub/device.map` und installieren Sie den Bootloader mit dem folgenden Befehl neu:

```
grub --batch < /etc/grub.conf
```

Windows von der zweiten Festplatte booten
: Einige Betriebssysteme, z. B. Windows, können nur von der ersten Festplatte gebootet werden. Wenn ein solches Betriebssystem auf einer anderen als der ersten Festplatte installiert ist, können Sie für den entsprechenden Menüeintrag einen logischen Tausch veranlassen.

```
...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

  In diesem Beispiel soll Windows von der zweiten Festplatte gestartet werden. Zu diesem Zweck wird die logische Reihenfolge der Festplatten mit `map` getauscht. Die Logik innerhalb der GRUB-Menüdatei ändert sich dadurch jedoch nicht. Daher müssen Sie bei `chainloader` nach wie vor die zweite Festplatte angeben.

12.7 Weiterführende Informationen

Umfassende Informationen zu GRUB finden Sie unter http://www.gnu.org/software/grub/. Ausführliche Informationen finden Sie auch auf der Infoseite für den Befehl `grub`. Weitere Informationen zu bestimmten Themen erhalten Sie auch,

wenn Sie „GRUB “ in der Suchfunktion für technische Informationen unter http://www.novell.com/support als Suchwort eingeben.



UEFI (Unified Extensible Firmware Interface) 13

Die UEFI (Unified Extensible Firmware Interface) bildet die Schnittstelle zwischen der Firmware, die sich auf der Systemhardware befindet, allen Hardware-Komponenten des Systems und dem Betriebssystem.

UEFI wird auf PC-Systemen immer stärker verbreitet und ersetzt allmählich das bisherige PC-BIOS. UEFI bietet beispielsweise echte Unterstützung für 64-Bit-Systeme und ermöglicht das sichere Booten („Secure Boot“, Firmware-Version 2.3.1c oder höher erforderlich), eine der zentralen Funktionen dieser Schnittstelle. Nicht zuletzt stellt UEFI auf allen x86-Plattformen eine Standard-Firmware bereit.

UEFI eröffnet außerdem die folgenden Vorteile:

- Booten von großen Festplatten (mehr als 2 TiB) mithilfe einer GUID-Partitionstabelle (GPT).
- CPU-unabhängige Architektur und Treiber.
- Flexible Vor-OS-Umgebung mit Netzwerkfunktionen.
- CSM (Compatibility Support Module) zur Unterstützung des Bootens älterer Betriebssysteme über eine PC-BIOS-ähnliche Emulation.

Weitere Informationen finden Sie unter `http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface`. Die nachfolgenden Abschnitte sollen keinen allgemeinen Überblick über UEFI liefern, sondern sie weisen lediglich darauf hin, wie bestimmte Funktionen in SUSE Linux Enterprise implementiert sind.

13.1 Secure Boot

Bei UEFI bedeutet die Absicherung des Bootstrapping-Prozesses, dass eine Vertrauenskette aufgebaut wird. Die „Plattform“ ist die Grundlage dieser Vertrauenskette; im SUSE Linux Enterprise-Kontext bilden die Hauptplatine und die On-Board-Firmware diese „Plattform“. Anders gesagt ist dies der Hardware-Hersteller, und die Vertrauenskette erstreckt sich von diesem Hardware-Hersteller zu den Komponentenherstellern, den Betriebssystemherstellern usw.

Das Vertrauen wird durch die Verschlüsselung mit öffentlichen Schlüsseln ausgedrückt. Der Hardware-Hersteller integriert einen sogenannten Plattformschlüssel (Platform Key, PK) in die Firmware, der die Grundlage für das Vertrauen legt. Das Vertrauensverhältnis zu Betriebssystemherstellern und anderen Dritten wird dadurch dokumentiert, dass ihre Schlüssel mit dem PK signiert werden.

Zum Gewährleisten der Sicherheit wird schließlich verlangt, dass die Firmware erst dann einen Code ausführt, wenn dieser Code mit einem dieser „verbürgten“ Schlüssel signiert ist – ein OS-Bootloader, ein Treiber im Flash-Speicher einer PCI-Express-Karte oder auf der Festplatte oder auch eine Aktualisierung der Firmware selbst.

Wenn Sie Secure Boot nutzen möchten, muss der OS-Loader also in jedem Fall mit einem Schlüssel signiert sein, der für die Firmware als verbürgt gilt, und der OS-Loader muss überprüfen, ob der zu ladende Kernel ebenfalls verbürgt ist.

In die UEFI-Schlüsseldatenbank können KEKs (Key Exchange Keys) aufgenommen werden. Auf diese Weise können Sie auch andere Zertifikate nutzen, sofern diese mit dem privaten Teil des PK signiert sind.

13.1.1 Implementation unter SUSE Linux Enterprise

Standardmäßig wird der KEK (Key Exchange Key) von Microsoft installiert.

ANMERKUNG: GUID-Partitionstabelle (GPT) erforderlich

Für die Secure Boot-Funktion ist eine GUID-Partitionstabelle (GPT) erforderlich, die die bisherige Partitionierung per MBR (Master Boot Record) ersetzt.

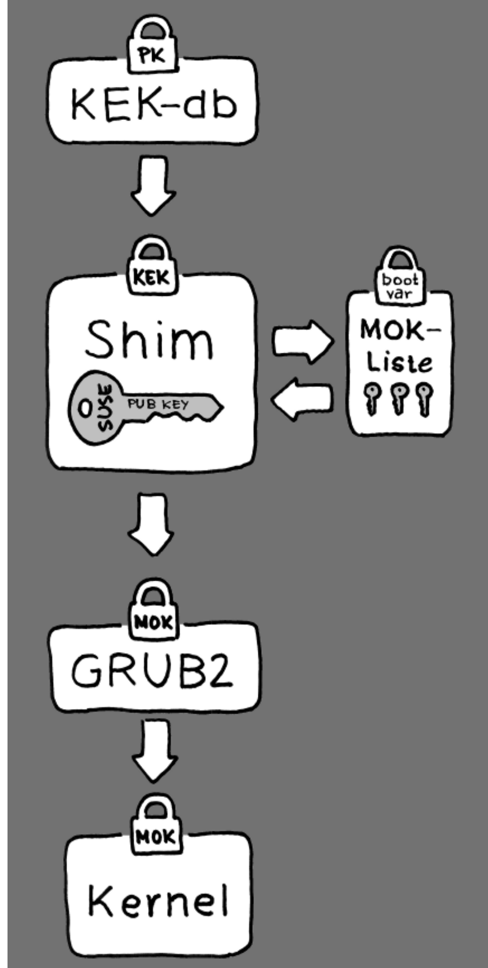
Wenn YaST während der Installation den EFI-Modus feststellt, wird versucht, eine GPT-Partition zu erstellen. UEFI erwartet die EFI-Programme auf einer FAT-formatierten ESP (EFI-Systempartition).

Zur Unterstützung von UEFI Secure Boot ist im Wesentlichen ein Bootloader mit einer digitalen Signatur erforderlich, den die Firmware als verbürgten Schlüssel erkennt. Zum Vorteil für SUSE Linux Enterprise-Kunden gilt dieser Schlüssel für die Firmware von vornherein als verbürgt, ohne dass der Benutzer manuell eingreifen müsste.

Hierzu gibt es zwei Möglichkeiten. Die erste Möglichkeit ist die Zusammenarbeit mit Hardware-Herstellern, sodass diese einen SUSE-Schlüssel zulassen, mit dem dann der Bootloader signiert wird. Die zweite Möglichkeit besteht darin, das Windows Logo Certification-Programm von Microsoft zu durchlaufen, damit der Bootloader zertifiziert wird und Microsoft den SUSE-Signierschlüssel anerkennt (also mit dem KEK von Microsoft signiert). Bislang wurde der Loader für SUSE vom UEFI Signing Service (in diesem Fall von Microsoft) signiert.



Abbildung 13.1 *UEFI: Secure Boot-Vorgang*



In der Implementierungsschicht nutzt SUSE den `shim`-Loader. Durch diese elegante Lösung werden rechtliche Probleme vermieden, und der Zertifizierungs- und Signierungsschritt wird erheblich vereinfacht. Der `shim`-Loader lädt einen Bootloader wie ELILO oder GRUB 2 und überprüft diesen Loader; der Bootloader wiederum lädt ausschließlich Kernels, die mit einem SUSE-Schlüssel signiert sind. SUSE bietet diese Funktion ab SLE11 SP3 in Neuinstallationen, in denen UEFI Secure Boot aktiviert ist.

Es gibt zwei Typen von verbürgten Benutzern.

- Erstens: Benutzer, die die Schlüssel besitzen. Der PK (Platform Key) ermöglicht nahezu alle Aktionen. Der KEK (Key Exchange Key) ermöglicht dieselben Aktionen wie ein PK, mit der Ausnahme, dass der PK hiermit nicht geändert werden kann.

- Zweitens: Benutzer mit physischem Zugang zum Computer. Ein Benutzer mit physischem Zugang kann den Computer neu booten und UEFI konfigurieren.

UEFI bietet zwei Arten von Variablen für die Anforderungen dieser Benutzer:

- Die ersten Variablen werden als „Authenticated Variables" (authentifizierte Variablen) bezeichnet. Diese Variablen können sowohl innerhalb des Bootvorgangs (in der sogenannten Boot Services Environment) und im laufenden Betriebssystem aktualisiert werden, jedoch nur dann, wenn der neue Wert der Variable mit demselben Schlüssel signiert ist wie der bisherige Wert. Zudem können diese Variablen nur an einen Wert mit einer höheren Seriennummer angehängt oder in einen Wert mit einer höheren Seriennummer geändert werden.

- Die zweiten Variablen sind die sogenannten „Boot Services Only Variables" (Variablen für Boot-Services). Diese Variablen stehen jedem Code zur Verfügung, der während des Bootvorgangs ausgeführt wird. Nach Abschluss des Bootvorgangs und vor dem Starten des Betriebssystems muss der Bootloader den Aufruf `ExitBootServices` auslösen. Anschließend sind diese Variablen nicht mehr zugänglich, und das Betriebssystem kann nicht mehr darauf zugreifen.

Die verschiedenen UEFI-Schlüssellisten sind vom ersten Typ, da es damit möglich ist, die Schlüssel, Treiber und Firmware-Fingerabdrücke online zu aktualisieren, hinzuzufügen und in Schwarze Listen einzutragen. Der zweite Variablentyp, also die „Boot Services Only Variables", unterstützt die Implementierung von Secure Boot auf sichere, Open Source-freundliche und damit GPLv3-kompatible Weise.

SUSE startet mit `shim`, einem kleinen, einfachen EFI-Bootloader, der ursprünglich von Fedora entwickelt wurde. Der Loader ist mit einem durch den SUSE-KEK signierten Zertifikat sowie mit einem von Microsoft ausgegebenen Zertifikat signiert, auf dessen Grundlage die KEKs in der UEFI-Schlüsseldatenbank im System zur Verfügung stehen.

Damit kann `shim` geladen und ausgeführt werden.

Anschließend überprüft `shim`, ob der zu ladende Bootloader verbürgt ist. In der Standardsituation verwendet `shim` ein unabhängiges SUSE-Zertifikat, das in diesen Loader

integriert ist. Darüber hinaus ermöglicht `shim` das „Registrieren“ weiterer Schlüssel, die Vorrag vor dem SUSE-Standardschlüssel erhalten. Im Folgenden werden diese Schlüssel als MOKs („Machine Owner Keys“) bezeichnet.

Danach überprüft und bootet der Bootloader den Kernel, und der Kernel überprüft und bootet seinerseits die Module.

13.1.2 MOK (Machine Owner Key)

Wenn der Benutzer (der „Machine Owner“, also der Eigentümer des Computers) eine Komponente im Bootvorgang ersetzen möchte, müssen MOKs (Machine Owner Keys) verwendet werden. Das Werkzeug `mokutils` hilft beim Signieren der Komponenten und beim Verwalten der MOKs.

Der Registrierungsvorgang beginnt mit dem Neubooten des Computers und dem Unterbrechen des Bootvorgangs (z. B. durch Drücken einer Taste), wenn `shim` geladen wird. `shim` geht dann in den Registrierungsmodus über, und der Benutzer kann den SUSE-Standardschlüssel durch Schlüssel aus einer Datei auf der Bootpartition ersetzen. Auf Wunsch des Benutzers kann `shim` dann einen Hash dieser Datei berechnen und das Ergebnis in einer „Boot Services Only“-Variable ablegen. Damit ist `shim` in der Lage, Änderungen an der Datei zu erkennen, die außerhalb der Boot-Services vorgenommen wurden; so wird eine Manipulation der Liste der benutzergenehmigten MOKs unterbunden.

Diese Vorgänge laufen zum Zeitpunkt des Bootens ab – nunmehr wird nur überprüfter Code ausgeführt. Daher kann nur ein Benutzer, der direkt an der Konsole sitzt, die Schlüssel des Computereigentümers verwenden. Bei Malware oder bei einem Hacker mit Fernzugriff auf das Betriebssystem ist dies nicht möglich, da Hacker und Malware lediglich die Datei ändern können, nicht jedoch den Hash, der in der „Boot Services Only“-Variable gespeichert ist.

Nach dem Laden und Überprüfen durch `shim` ruft der Bootloader wiederum `shim` auf, um den Kernel zu überprüfen. So wird eine Duplizierung des Prüfcodes vermieden. `shim` greift hierzu auf dieselbe MOK-Liste zu und teilt dem Bootloader mit, ob der Kernel geladen weden kann.

Auf diese Weise können Sie Ihren eigenen Kernel oder Bootloader installieren. Sie müssen lediglich einen neuen Schlüsselsatz installieren und im Rahmen Ihrer physischen Anwesenheit beim ersten Neubooten bestätigen. Es gibt nicht nur einen MOK, sondern

eine ganze MOK-Liste. Aus diesem Grund kann `shim` die Schlüssel von verschiedenen Herstellern als verbürgt betrachten, sodass auch Dual-Boot- und Multi-Boot-Funktionen mit dem Bootloader möglich sind.

13.1.3 Booten eines benutzerdefinierten Kernels

Die folgenden Ausführungen beruhen auf http://en.opensuse.org/openSUSE:UEFI#Booting_a_custom_kernel.

Secure Boot verhindert nicht die Nutzung eines selbst kompilierten Kernels. Sie müssen den Kernel mit Ihrem eigenen Zertifikat signieren und dieses Zertifikat für die Firmware oder den MOK bekanntgeben.

1. Erstellen Sie einen benutzerdefinierten X.509-Schlüssel und ein entsprechendes Zertifikat für die Signierung:

   ```
   openssl req -new -x509 -newkey rsa:2048 -keyout key.asc \
     -out cert.pem -nodes -days 666 -subj "/CN=$USER/"
   ```

   Weitere Informationen zum Erstellen von Zertifikaten finden Sie unter http://en.opensuse.org/openSUSE:UEFI_Image_File_Sign_Tools#Create_Your_Own_Certificate.

2. Verpacken Sie den Schlüssel und das Zertifikat als PKCS#12-Struktur:

   ```
   openssl pkcs12 -export -inkey key.asc -in cert.pem \
     -name kernel_cert -out cert.p12
   ```

3. Generieren Sie eine NSS-Datenbank für `pesign`:

   ```
   certutil -d . -N
   ```

4. Importieren Sie den Schlüssel und das Zertifikat aus PKCS#12 in die NSS-Datenbank:

   ```
   pk12util -d . -i cert.p12
   ```

5. „Authentifizieren“ Sie den Kernel mit der neuen Signatur mithilfe von `pesign`:

   ```
   pesign -n . -c kernel_cert -i arch/x86/boot/bzImage \
     -o vmlinuz.signed -s
   ```

6 Listen Sie die Signaturen im Kernel-Image auf:

```
pesign -n . -S -i vmlinuz.signed
```

Zu diesem Zeitpunkt können Sie den Kernel wie gewohnt in `/boot` installieren. Der Kernel besitzt nun eine benutzerdefinierte Signatur, sodass das Zertifikat zum Signieren in die UEFI-Firmware oder in den MOK importiert werden muss.

7 Konvertieren Sie das Zertifikat zum Importieren in die Firmware oder den MOK in das DER-Format:

```
openssl x509 -in cert.pem -outform der -out cert.der
```

8 Kopieren Sie das Zertifikat aus Gründen des einfacheren Zugriffs in die ESP:

```
sudo cp cert.der /boot/efi/
```

9 Mit `mokutil` wird die MOK-Liste automatisch gestartet.

Zum manuellen Starten des MOK gehen Sie alternativ wie folgt vor:

9a Booten Sie den Computer neu

9b Drücken Sie im GRUB -Menü die Taste „`c`“.

9c Typ:

```
chainloader $efibootdir/MokManager.efi
boot
```

9d Wählen Sie *Enroll key from disk (Schlüssel von Festplatte registrieren)*.

9e Navigieren Sie zur Datei `cert.der`, und drücken Sie die Eingabetaste.

9f Registrieren Sie den Schlüssel gemäß den Anweisungen. In der Regel drücken Sie hierzu „`0`“ und dann zum Bestätigen „`j`“.

Alternativ können Sie einen neuen Schlüssel über das Firmware-Menü in die Signaturdatenbank aufnehmen.

13.1.4 Verwenden von Nicht-Inbox-Treibern

Das Hinzufügen von Nicht-Inbox-Treibern (also Treiber, die nicht in SLE inbegriffen sind) wird nach dem Booten in die Installation mit aktiviertem Secure Boot nicht unterstützt. Der Signierschlüssel für SolidDriver/PLDP gilt standardmäßig nicht als vertrauenswürdig.

Es ist jedoch mit zwei Methoden möglich, Treiber von Drittanbietern bei der Installation mit aktiviertem Secure Boot zu nutzen:

- Fügen Sie die erforderlichen Schlüssel vor der Installation mithilfe von Firmware-/Systemverwaltungswerkzeugen in die Firmware-Datenbank ein. Diese Option ist von der jeweils verwendeten Hardware abhängig. Weitere Informationen erhalten Sie bei Ihrem Hardware-Händler.

- Verwenden Sie ein bootfähiges Treiber-ISO-Image von `https://drivers.suse.com/` oder von Ihrem Hardware-Händler, mit dem die erforderlichen Schlüssel beim ersten Starten in die MOK-Liste eingetragen werden.

So tragen Sie die Treiberschlüssel mit dem bootfähigen Treiber-ISO-Image in die MOK-Liste ein:

1. Brennen Sie das ISO-Image auf eine leere CD/DVD.

2. Starten Sie die Installation. Booten Sie hierzu von der neuen CD/DVD und halten Sie dabei die standardmäßigen SUSE Linux Enterprise-Medien bzw. die URL zu einem Netzwerkinstallationsserver bereit.

   Wenn Sie eine Netzwerkinstallation vornehmen, geben Sie die URL der Netzwerkinstallationsquelle mit der Option `install=` in die Bootbefehlszeile ein.

   Bei einer Installation von optischen Speichermedien bootet das Installationsprogramm zunächst vom Treiber-Kit; anschließend werden Sie aufgefordert, den ersten Datenträger für SUSE Linux Enterprise einzulegen.

3. Bei der Installation wird ein initrd mit aktualisierten Treibern herangezogen.

Weitere Informationen finden Sie unter `https://drivers.suse.com/doc/Usage/Secure_Boot_Certificate.html`.

13.1.5 Einschränkungen

Beim Booten im Secure Boot-Modus gelten die folgenden Einschränkungen:

- Hybridisierte ISO-Images werden auf UEFI-Systemen nicht als bootfähig erkannt. In SP3 wird daher das UEFI-Booten von USB-Geräten nicht unterstützt.
- Um zu gewährleisten, dass Secure Boot nicht einfach umgangen werden kann, sind einige Kernelfunktionen beim Ausführen unter Secure Boot deaktiviert.
- Der Bootloader, der Kernel und die Kernelmodule müssen signiert sein.
- kexec und kdump sind deaktiviert.
- Der Ruhezustand (Suspend on Disk) ist deaktiviert.
- Der Zugriff auf `/dev/kmem` und `/dev/mem` ist nicht möglich, auch nicht als Root-Benutzer.
- Der Zugriff auf den E/A-Anschluss ist nicht möglich, auch nicht als Root-Benutzer. Alle X11-Grafiktreiber müssen einen Kerneltreiber verwenden.
- Der PCI-BAR-Zugriff über sysfs ist nicht möglich.
- `custom_method` in ACPI ist nicht verfügbar.
- debugfs für das Modul asus-wmi ist nicht verfügbar.
- Der Parameter `acpi_rsdp` hat keine Auswirkungen auf den Kernel.

13.2 Weiterführende Informationen

- http://www.uefi.org – UEFI-Homepage mit den aktuellen UEFI-Spezifikationen.
- Blogeinträge von Olaf Kirch und Vojtěch Pavlík (das obige Kapitel ist stark auf diese Einträge gestützt):
  - http://www.suse.com/blogs/uefi-secure-boot-plan/

- http://www.suse.com/blogs/uefi-secure-boot-overview/
- http://www.suse.com/blogs/uefi-secure-boot-details/

- http://en.opensuse.org/openSUSE:UEFI – UEFI mit openSUSE.



14 Spezielle Systemfunktionen

In diesem Kapitel erhalten Sie zunächst Informationen zu den verschiedenen Softwarepaketen, zu den virtuellen Konsolen und zur Tastaturbelegung. Hier finden Sie Hinweise zu Software-Komponenten, wie `bash`, `cron` und `logrotate`, da diese im Laufe der letzten Veröffentlichungszyklen geändert oder verbessert wurden. Selbst wenn sie nur klein sind oder als nicht besonders wichtig eingestuft werden, können die Benutzer ihr Standardverhalten ändern, da diese Komponenten häufig eng mit dem System verbunden sind. Das Kapitel endet mit einem Abschnitt mit sprach- und landesspezifischen Einstellungen (I18N und L10N).

14.1 Informationen zu speziellen Softwarepaketen

Die Programme `bash`, `cron`, `logrotate`, `locate`, `ulimit` und `free` spielen für Systemadministratoren und viele Benutzer eine wichtige Rolle. man-Seiten und info-Seiten sind hilfreiche Informationsquellen zu Befehlen, sind jedoch nicht immer verfügbar. GNU Emacs ist ein beliebter konfigurierbarer Texteditor.

14.1.1 Das Paket bash und /etc/profile

Bash ist die Standard-System-Shell. Wenn sie als Anmelde-Shell verwendet wird, werden mehrere Initialisierungsdateien gelesen. Bash verarbeitet die entsprechenden Informationen in der Reihenfolge dieser Liste:

1. /etc/profile

2. ~/.profile

3. /etc/bash.bashrc

4. ~/.bashrc

Nehmen Sie benutzerdefinierte Einstellungen in ~/.profile oder ~/.bashrc vor. Um die richtige Verarbeitung der Dateien zu gewährleisten, müssen die Grundeinstellungen aus /etc/skel/.profile oder /etc/skel/.bashrc in das Home-Verzeichnis des Benutzers kopiert werden. Es empfiehlt sich, die Einstellungen aus /etc/skel nach einer Aktualisierung zu kopieren. Führen Sie die folgenden Shell-Befehle aus, um den Verlust persönlicher Einstellungen zu vermeiden:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Kopieren Sie anschließend die persönlichen Einstellungen erneut aus den *.old-Dateien.

14.1.2 Das cron-Paket

Wenn Sie Kommandos regelmäßig und automatisch zu bestimmten Zeiten im Hintergrund ausführen möchten, verwenden Sie dazu am besten das Tool cron. cron wird durch speziell formatierte Zeittabellen gesteuert. Einige sind bereits im Lieferumfang des Systems enthalten, bei Bedarf können Benutzer jedoch auch eigene Tabellen erstellen.

Die cron-Tabellen befinden sich im Verzeichnis /var/spool/cron/tabs. /etc/crontab dient als systemübergreifende cron-Tabelle. Geben Sie den Benutzernamen zur Ausführung des Befehls unmittelbar nach der Zeittabelle und noch vor dem Befehl ein. In Beispiel 14.1, „Eintrag in /etc/crontab“ (S. 190), wird root eingegeben. Die paketspezifischen Tabellen in /etc/cron.d weisen alle dasselbe Format auf. Informationen hierzu finden Sie auf der man-Seite zu cron (man cron).

Beispiel 14.1 *Eintrag in /etc/crontab*

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Sie können /etc/crontab nicht bearbeiten, indem Sie den Befehl crontab -e bearbeiten. Die Datei muss direkt in einem Editor geladen, geändert und dann gespeichert werden.

Einige Pakte installieren Shell-Skripten in die Verzeichnisse /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly und /etc/cron.monthly, deren Ausführung durch /usr/lib/cron/run-crons gesteuert wird. /usr/lib/cron/run-crons wird alle 15 Minuten von der Haupttabelle (/etc/crontab) ausgeführt. Hiermit wird gewährleistet, dass vernachlässigte Prozesse zum richtigen Zeitpunkt ausgeführt werden können.

Um die Skripten hourly, daily oder andere Skripten für regelmäßige Wartungsarbeiten zu benutzerdefinierten Zeiten auszuführen, entfernen Sie regelmäßig die Zeitstempeldateien mit /etc/crontab-Einträgen (siehe Beispiel 14.2, „/etc/crontab: Entfernen der Zeitstempeldateien" (S. 191) – u. a. wird hourly vor jeder vollen Stunde und daily einmal täglich um 2:14 Uhr entfernt).

Beispiel 14.2 */etc/crontab: Entfernen der Zeitstempeldateien*

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Sie können auch DAILY_TIME in /etc/sysconfig/cron auf die Zeit einstellen, zu der cron.daily gestartet werden soll. Mit MAX_NOT_RUN stellen Sie sicher, dass die täglichen Aufgaben auch dann ausgeführt werden, wenn der Computer zur angegebenen DAILY_TIME und auch eine längere Zeit danach nicht eingeschaltet ist. Die maximale Einstellung von MAX_NOT_RUN sind 14 Tage.

Die täglichen Systemwartungsaufträge werden zum Zwecke der Übersichtlichkeit auf mehrere Skripts verteilt. Sie sind im Paket aaa_base enthalten. /etc/cron.daily enthält beispielsweise die Komponenten suse.de-backup-rpmdb, suse.de-clean-tmp oder suse.de-cron-local.

14.1.3 Protokolldateien: Paket logrotate

Mehrere Systemdienste (*Dämonen*) zeichnen zusammen mit dem Kernel selbst regelmäßig den Systemstatus und spezielle Ereignisse in Protokolldateien auf. Auf diese Weise kann der Administrator den Status des Systems zu einem bestimmten Zeitpunkt

regelmäßig überprüfen, Fehler oder Fehlfunktionen erkennen und die Fehler mit Präzision beheben. Die Protokolldateien werden in der Regel, wie von FHS angegeben, unter /var/log gespeichert und werden täglich umfangreicher. Mit dem Paket logrotate kann der Umfang der Dateien gesteuert werden.

Konfigurieren Sie Logrotate mit der Datei /etc/logrotate.conf. Die Dateien, die zusätzlich gelesen werden sollen, werden insbesondere durch die include-Spezifikation konfiguriert. Programme, die Protokolldateien erstellen, installieren einzelne Konfigurationsdateien in /etc/logrotate.d. Solche Dateien sind beispielsweise im Lieferumfang der Pakete apache2 (/etc/logrotate.d/apache2) und syslogd (/etc/logrotate.d/syslogd) enthalten.

Beispiel 14.3 *Beispiel für /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotate wird über cron gesteuert und täglich durch /etc/cron.daily/logrotate aufgerufen.

WICHTIG

Mit der Option `create` werden alle vom Administrator in `/etc/permissions*` vorgenommenen Einstellungen gelesen. Stellen Sie sicher, dass durch persönliche Änderungen keine Konflikte auftreten.

14.1.4 Der Befehl „locate“

`locate`, ein Kommando zum schnellen Suchen von Dateien, ist nicht im Standardumfang der installierten Software enthalten. Wenn Sie möchten, installieren Sie das Paket `findutils-locate`. Der Prozess updatedb wird jeden Abend etwa 15 Minuten nach dem Booten des Systems gestartet.

14.1.5 Der Befehl „ulimit“

Mit dem Kommando `ulimit` (*user limits*) ist es möglich, Begrenzungen für die Verwendung von Systemressourcen festzulegen und anzuzeigen. `ulimit` ist besonders nützlich für die Begrenzung des verfügbaren Arbeitsspeichers für Anwendungen. Damit kann eine Anwendung daran gehindert werden, zu viele Systemressourcen zu reservieren und damit das Betriebssystem zu verlangsamen oder sogar aufzuhängen.

`ulimit` kann mit verschiedenen Optionen verwendet werden. Verwenden Sie zum Begrenzen der Speicherauslastung die in Tabelle 14.1, „`ulimit`: Einstellen von Ressourcen für Benutzer“ (S. 193) aufgeführten Optionen.

Tabelle 14.1 *ulimit: Einstellen von Ressourcen für Benutzer*

`-m`	Die maximale nicht auslagerbare festgelegte Größe
`-v`	Die maximale Größe des virtuellen Arbeitsspeichers, der der Shell zur Verfügung steht
`-s`	Die maximale Größe des Stapels

`-c`	Die maximale Größe der erstellten Kerndateien
`-a`	Alle aktuellen Grenzwerte werden gemeldet

In `/etc/profile` können Sie systemweite Einträge vornehmen. Aktivieren Sie hier die Erstellung der Core-Dateien, die Programmierer für die *Fehlersuche* benötigen. Ein normaler Benutzer kann die in `/etc/profile` vom Systemadministrator festgelegten Werte nicht erhöhen, er kann jedoch spezielle Einträge in `~/.bashrc` vornehmen.

Beispiel 14.4 *ulimit: Einstellungen in ~/.bashrc*

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

Die Speicherzuteilungen müssen in KB erfolgen. Weitere Informationen erhalten Sie mit `man bash`.

WICHTIG

`ulimit`-Direktiven werden nicht von allen Shells unterstützt. PAM (beispielsweise `pam_limits`) bietet umfassende Anpassungsmöglichkeiten, wenn Sie Einstellungen für diese Beschränkungen vornehmen müssen.

14.1.6 Der Befehl „free“

Dasommando `free` zeigt die Größe des insgesamt vorhandenen freien und verwendeten physischen Arbeitsspeichers und Auslagerungsspeichers im System sowie die vom Kernel verwendeten Puffer und den verwendeten Cache an. Das Konzept des *verfügbaren Arbeitsspeichers* geht auf Zeiten vor der einheitlichen Speicherverwaltung zurück. Bei Linux gilt der Grundsatz *freier Arbeitsspeicher ist schlechter Arbeitsspeicher.* Daher wurde bei Linux immer darauf geachtet, die Caches auszugleichen, ohne freien oder nicht verwendeten Arbeitsspeicher zuzulassen.

Der Kernel verfügt nicht direkt über Anwendungs- oder Benutzerdaten. Stattdessen verwaltet er Anwendungen und Benutzerdaten in einem *Seiten-Cache*. Falls nicht mehr

genügend Arbeitsspeicher vorhanden ist, werden Teile auf der Swap-Partition oder in Dateien gespeichert, von wo aus sie mithilfe des Befehls `mmap` abgerufen werden können (siehe `man mmap`).

Der Kernel enthält zusätzlich andere Caches, wie beispielsweise den *slab-Cache*, in dem die für den Netzwerkzugriff verwendeten Caches gespeichert werden. Dies erklärt die Unterschiede zwischen den Zählern in `/proc/meminfo`. Die meisten, jedoch nicht alle dieser Zähler, können über `/proc/slabinfo` aufgerufen werden.

Wenn Sie jedoch herausfinden möchten, wie viel RAM gerade verwendet wird, dann finden Sie diese Information in `/proc/meminfo`.

14.1.7 man-Seiten und Info-Seiten

Für einige GNU-Anwendungen (wie beispielsweise tar) sind keine man-Seiten mehr vorhanden. Verwenden Sie für diese Befehle die Option `--help`, um eine kurze Übersicht über die info-Seiten zu erhalten, in der Sie detailliertere Anweisungen erhalten. info befindet sich im Hypertextsystem von GNU. Eine Einführung in dieses System erhalten Sie, wenn Sie `infoinfo` eingeben. Info-Seiten können mit Emacs angezeigt werden, wenn Sie `emacs -f info` eingeben oder mit `info` direkt in einer Konsole angezeigt werden. Sie können auch tkinfo, xinfo oder das Hilfesystem zum Anzeigen von info-Seiten verwenden.

14.1.8 Auswählen von man-Seiten über das Kommando man

Geben Sie `man` *`man_page`* ein, um die man-Seite zu lesen. Wenn bereits eine man-Seite mit demselben Namen in anderen Abschnitten vorhanden ist, werden alle vorhandenen Seiten mit den zugehörigen Abschnittsnummern aufgeführt. Wählen Sie die aus, die Sie anzeigen möchten. Wenn Sie innerhalb einiger Sekunden keine Abschnittsnummer eingeben, wird die erste Seite angezeigt.

Wenn Sie zum standardmäßigen Systemverhalten zurückkehren möchten, setzen Sie `MAN_POSIXLY_CORRECT=1` in einer Shell-Initialisierungsdatei wie `~/.bashrc`.

14.1.9 Einstellungen für GNU Emacs

GNU Emacs ist eine komplexe Arbeitsumgebung. In den folgenden Abschnitten werden die beim Starten von GNU Emacs verarbeiteten Dateien beschrieben. Weitere Informationen hierzu erhalten Sie online unter `http://www.gnu.org/software/emacs/`.

Beim Starten liest Emacs mehrere Dateien, in denen die Einstellungen für den Benutzer, den Systemadministrator und den Distributor zur Anpassung oder Vorkonfiguration enthalten sind. Die Initialisierungsdatei `~/.emacs` ist in den Home-Verzeichnissen der einzelnen Benutzer von `/etc/skel` installiert. `.emacs` wiederum liest die Datei `/etc/skel/.gnu-emacs`. Zum Anpassen des Programms kopieren Sie `.gnu-emacs` in das Home-Verzeichnis (mit `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) und nehmen Sie dort die gewünschten Einstellungen vor.

`.gnu-emacs` definiert die Datei `~/.gnu-emacs-custom` als `custom-file`. Wenn Benutzer in Emacs Einstellungen mit den `customize`-Optionen vornehmen, werden die Einstellungen in `~/.gnu-emacs-custom` gespeichert.

Bei SUSE Linux Enterprise Desktop wird mit dem `emacs`-Paket die Datei `site-start.el` im Verzeichnis `/usr/share/emacs/site-lisp` installiert. Die Datei `site-start.el` wird vor der Initialisierungsdatei `~/.emacs` geladen. Mit `site-start.el` wird unter anderem sichergestellt, dass spezielle Konfigurationsdateien mit Emacs-Zusatzpaketen, wie `psgml`, automatisch geladen werden. Konfigurationsdateien dieses Typs sind ebenfalls unter `/usr/share/emacs/site-lisp` gespeichert und beginnen immer mit `suse-start-`. Der lokale Systemadministrator kann systemweite Einstellungen in `default.el` festlegen.

Weitere Informationen zu diesen Dateien finden Sie in der Info-Datei zu Emacs unter *Init File:* `info:/emacs/InitFile`. Informationen zum Deaktivieren des Ladens dieser Dateien (sofern erforderlich) stehen dort ebenfalls zur Verfügung.

Die Komponenten von Emacs sind in mehrere Pakete unterteilt:

- Das Basispaket `emacs`.
- `emacs-x11` (in der Regel installiert): das Programm *mit* X11-Support.

- emacs-nox: das Programm *ohne* X11-Support.
- emacs-info: Online-Dokumentation im info-Format.
- emacs-el: die nicht kompilierten Bibliotheksdateien in Emacs Lisp. Sie sind während der Laufzeit nicht erforderlich.
- Verschiedene Add-On-Pakete können bei Bedarf installiert werden: emacs-auctex (LaTeX), psgml (SGML und XML), gnuserv (Client- und Server-Vorgänge) und andere.

14.2 Virtuelle Konsolen

Linux ist ein Multitasking-System für den Mehrbenutzerbetrieb. Die Vorteile dieser Funktionen können auch auf einem eigenständigen PC-System genutzt werden. Im Textmodus stehen sechs virtuelle Konsolen zur Verfügung. Mit den Tastenkombinationen Alt + F1 bis Alt + F6 können Sie zwischen den Konsolen umschalten. Die siebte Konsole ist für X und reserviert und in der zehnten Konsole werden Kernel-Meldungen angezeigt. Durch Ändern der Datei /etc/inittab können mehrere oder weniger Konsolen zugewiesen werden.

Wenn Sie von X ohne Herunterfahren zu einer anderen Konsole wechseln möchten, verwenden Sie die Tastenkombinationen Strg + Alt + F1 bis Strg + Alt + F6. Mit Alt + F7 kehren Sie zu X zurück.

14.3 Tastaturzuordnung

Um die Tastaturzuordnung der Programme zu standardisieren, wurden Änderungen an folgenden Dateien vorgenommen:

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.emacs
/etc/skel/.gnu-emacs
/etc/skel/.vimrc
/etc/csh.cshrc
/etc/termcap
/usr/share/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Diese Änderungen betreffen nur Anwendungen, die terminfo-Einträge verwenden oder deren Konfigurationsdateien direkt geändert werden (vi, emacs usw.). Anwendungen, die nicht im Lieferumfang des Systems enthalten sind, sollten an diese Standards angepasst werden.

Unter X kann die Compose-Taste (Multi-Key) gemäß /etc/X11/Xmodmap aktiviert werden.

Weitere Einstellungen sind mit der X-Tastaturerweiterung (XKB) möglich. Diese Erweiterung wird auch von den Desktop-Umgebungen GNOME (gswitchit) und KDE (kxkb) verwendet.

TIPP: Weiterführende Informationen

Informationen zu XKB finden Sie in den Dokumenten, die unter /usr/share/doc/packages/xkeyboard-config (Teil des Pakets xkeyboard-config) aufgelistet sind.

14.4 Sprach- und länderspezifische Einstellungen

Das System wurde zu einem großen Teil internationalisiert und kann an lokale Gegebenheiten angepasst werden. Die Internationalisierung (*I18N*) ermöglicht spezielle Lokalisierungen (*L10N*). Die Abkürzungen I18N und L10N wurden von den ersten und letzten Buchstaben der englischsprachigen Begriffe und der Anzahl der dazwischen stehenden ausgelassenen Buchstaben abgeleitet.

Die Einstellungen werden mit LC_-Variablen vorgenommen, die in der Datei /etc/sysconfig/language definiert sind. Dies bezieht sich nicht nur auf die *native Sprachunterstützung* , sondern auch auf die Kategorien *Meldungen* (Sprache) *Zeichensatz*, *Sortierreihenfolge*, *Uhrzeit und Datum*, *Zahlen* und *Währung*. Diese Kategorien können direkt über eine eigene Variable oder indirekt mit einer Master-Variable in der Datei language festgelegt werden (weitere Informationen erhalten Sie auf der man-Seite zu locale).

RC_LC_MESSAGES, RC_LC_CTYPE, RC_LC_COLLATE, RC_LC_TIME, RC_LC_NUMERIC, RC_LC_MONETARY
: Diese Variablen werden ohne das Präfix RC_ an die Shell weitergegeben und stehen für die aufgelisteten Kategorien. Die betreffenden Shell-Profile werden unten aufgeführt. Die aktuelle Einstellung lässt sich mit dem Befehl locale anzeigen.

RC_LC_ALL
: Sofern diese Variable festgelegt ist, setzt Sie die Werte der bereits erwähnten Variablen außer Kraft.

RC_LANG
: Falls keine der zuvor genannten Variablen festgelegt ist, ist dies das Fallback. Standardmäßig wird nur RC_LANG festgelegt. Dadurch wird es für die Benutzer einfacher, eigene Werte einzugeben.

ROOT_USES_LANG
: Eine Variable, die entweder den Wert yes oder den Wert no aufweist. Wenn die Variable auf no gesetzt ist, funktioniert root immer in der POSIX-Umgebung.

Die Variablen können über den sysconfig-Editor von YaST (siehe Abschnitt 11.3.1, „Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"“ (S. 146)) festgelegt werden. Der Wert einer solchen Variable enthält den Sprachcode, den Ländercode, die Codierung und einen Modifier. Die einzelnen Komponenten werden durch Sonderzeichen verbunden:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

14.4.1 Beispiele

Sprach- und Ländercode sollten immer gleichzeitig eingestellt werden. Die Spracheinstellungen entsprechen der Norm ISO 639, die unter http://www.evertype.com/standards/iso639/iso639-en.html und http://www.loc.gov/standards/iso639-2/ verfügbar ist. Die Ländercodes sind in ISO 3166 aufgeführt (siehe http://en.wikipedia.org/wiki/ISO_3166).

Es ist nur sinnvoll, Werte festzulegen, für die verwendbare Beschreibungsdateien unter /usr/lib/locale zu finden sind. Anhand der Dateien in /usr/share/i18n können mit dem Befehl localedef zusätzliche Beschreibungsdateien erstellt werden.

Die Beschreibungsdateien sind Bestandteil des Pakets glibc-i18ndata. Eine Beschreibungsdatei für en_US.UTF-8 (für Englisch und USA) kann beispielsweise wie folgt erstellt werden:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

LANG=en_US.UTF-8
: Dies ist die Standardeinstellung, wenn während der Installation US-Englisch ausgewählt wurde. Wenn Sie eine andere Sprache ausgewählt haben, wird diese Sprache ebenfalls mit der Zeichencodierung UTF-8 aktiviert.

LANG=en_US.ISO-8859-1
: Hiermit wird als Sprache Englisch, als Land die USA und als Zeichensatz ISO-8859-1 festgelegt. In diesem Zeichensatz wird das Eurozeichen nicht unterstützt, es kann jedoch gelegentlich in Programmen nützlich sein, die nicht für die UTF-8-Unterstützung aktualisiert wurden. Die Zeichenkette, mit der der Zeichensatz definiert wird (in diesem Fall ISO-8859-1), wird anschließend von Programmen, wie Emacs, ausgewertet.

LANG=en_IE@euro
: Im oben genannten Beispiel wird das Eurozeichen explizit in die Spracheinstellung aufgenommen. Diese Einstellung ist nun grundsätzlich überflüssig, da UTF-8 auch das Eurosymbol enthält. Sie ist nur nützlich, wenn eine Anwendung ISO-8859-15 anstelle von UTF-8 unterstützt.

In früheren Versionen war es erforderlich, SuSEconfig im Anschluss an alle Änderungen an /etc/sysconfig/language auszuführen. SuSEconfig hat die Änderungen dann in /etc/SuSEconfig/profile und /etc/SuSEconfig/csh.login geschrieben. Bei der Anmeldung wurden diese Dateien durch /etc/profile (für die Bash-Shell) oder durch /etc/csh.login (für tcsh) gelesen.

In den aktuellen Versionen wurde /etc/SuSEconfig/profile durch /etc/profile.d/lang.sh und /etc/SuSEconfig/csh.login durch /etc/profile.de/lang.csh ersetzt. Wenn sie jedoch vorhanden sind, werden beide alten Dateien bei der Anmeldung weiterhin gelesen.

Der Prozessablauf sieht nun wie folgt aus:

- Für die Bash: /etc/profile liest /etc/profile.d/lang.sh, die ihrerseits /etc/sysconfig/language analysiert.

- Für tcsh: /etc/profile liest /etc/profile.d/lang.csh, die ihrerseits /etc/sysconfig/language analysiert.

So wird sichergestellt, dass sämtliche Änderungen an /etc/sysconfig/language bei der nächsten Anmeldung in der entsprechenden Shell verfügbar sind, ohne dass zuerst SuSEconfig ausgeführt werden muss.

Die Benutzer können die Standardeinstellungen des Systems außer Kraft setzen, indem Sie die Datei ~/.bashrc entsprechend bearbeiten. Wenn Sie die systemübergreifende Einstellung en_US für Programmmeldungen beispielsweise nicht verwenden möchten, nehmen Sie beispielsweise LC_MESSAGES=es_ES auf, damit die Meldungen stattdessen auf Spanisch angezeigt werden.

14.4.2 Locale-Einstellungen in ~/.i18n

Wenn Sie mit den Locale-Systemstandardwerten nicht zufrieden sind, können Sie die Einstellungen in ~/.i18n ändern. Achten Sie dabei jedoch auf die Einhaltung der Bash-Scripting-Syntax. Die Einträge in ~/.i18n setzen die Systemstandardwerte aus /etc/sysconfig/language außer Kraft. Verwenden Sie dieselben Variablennamen, jedoch ohne die RC_-Präfixe für den Namespace, also beispielsweise LANG anstatt RC_LANG:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

14.4.3 Einstellungen für die Sprachunterstützung

Die Dateien in der Kategorie *Meldungen* werden generell im entsprechenden Sprachverzeichnis (wie beispielsweise en) gespeichert, damit ein Fallback vorhanden ist. Wenn Sie für LANG den Wert en_US festlegen und in /usr/share/locale/en_US/LC_MESSAGES keine Meldungsdatei vorhanden ist, wird ein Fallback auf /usr/share/locale/en/LC_MESSAGES ausgeführt.

Darüber hinaus kann eine Fallback-Kette definiert werden, beispielsweise für Bretonisch zu Französisch oder für Galizisch zu Spanisch oder Portugiesisch:

`LANGUAGE=„br_FR:fr_Fr“`

`LANGUAGE=„gl_ES:es_ES:pt_PT“`

Wenn Sie möchten, können Sie die norwegischen Varianten Nynorsk und Bokmål (mit zusätzlichem Fallback auf `no`) verwenden:

`LANG=„nn_NO“`

`LANGUAGE=„nn_NO:nb_NO:no“`

oder

`LANG=„nb_NO“`

`LANGUAGE=„nb_NO:nn_NO:no“`

Beachten Sie, das bei Norwegisch auch `LC_TIME` anders behandelt wird.

Ein mögliches Problem ist, dass ein Trennzeichen, das zum Trennen von Zifferngruppen verwendet wird, nicht richtig erkannt wird. Dies passiert, wenn `LANG` auf einen aus zwei Buchstaben bestehenden Sprachcode wie `de` eingestellt ist, die Definitionsdatei, die glibc verwendet, jedoch in `/usr/share/lib/de_DE/LC_NUMERIC` gespeichert ist. Daher muss `LC_NUMERIC` auf `de_DE` gesetzt sein, damit das System die Trennzeichendefinition erkennen kann.

14.4.4 Weiterführende Informationen

- *The GNU C Library Reference Manual*, Kapitel „Locales and Internationalization“. Dieses Handbuch ist in `glibc-info` enthalten. Das Paket befindet sich im SUSE Linux Enterprise-SDK (Software Development Kit). Das SDK ist ein Add-on-Produkt für SUSE Linux Enterprise und ist unter `http://download.suse.com/` als Download verfügbar.

- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, momentan verfügbar unter `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.

- *Unicode-Howto* von Bruno Haible, verfügbar unter `http://tldp.org/HOWTO/Unicode-HOWTO-1.html`.



Druckerbetrieb 15

SUSE® Linux Enterprise Desktop unterstützt zahlreiche Druckermodelle (auch entfernte Netzwerkdrucker). Drucker können manuell oder mit YaST konfiguriert werden. Anleitungen zur Konfiguration finden Sie unter Abschnitt „Einrichten eines Druckers“ (Kapitel 5, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Bereitstellungshandbuch*). Grafische Dienstprogramme und Dienstprogramme an der Kommandozeile sind verfügbar, um Druckaufträge zu starten und zu verwalten. Wenn Ihr Drucker nicht wie erwartet verwendet werden kann, lesen Sie die Informationen unter Abschnitt 15.7, „Fehlersuche“ (S. 215).

Das Standarddrucksystem in SUSE Linux Enterprise Desktop ist CUPS (Common Unix Printing System).

Drucker können nach Schnittstelle, z. B. USB oder Netzwerk, und nach Druckersprache unterschieden werden. Stellen Sie beim Kauf eines Druckers sicher, dass der Drucker über eine für Ihre Hardware geeignete Schnittstelle (wie USB oder einen parallelen Port) und eine geeignete Druckersprache verfügt. Drucker können basierend auf den folgenden drei Klassen von Druckersprachen kategorisiert werden:

PostScript-Drucker
: PostScript ist die Druckersprache, in der die meisten Druckaufträge unter Linux und Unix vom internen Drucksystem generiert und verarbeitet werden. Wenn PostScript-Dokumente direkt vom Drucker verarbeitet und im Drucksystem nicht in weiteren Phasen konvertiert werden müssen, reduziert sich die Anzahl der möglichen Fehlerquellen.

Standarddrucker (Sprachen wie PCL und ESC/P)
: Obwohl diese Druckersprachen ziemlich alt sind, werden sie immer weiter entwickelt, um neue Druckerfunktionen unterstützen zu können. Bei den bekannten Druckersprachen kann das Drucksystem PostScript-Druckaufträge mithilfe von Ghostscript in die entsprechende Druckersprache konvertieren. Diese Verarbeitungsphase wird als „Interpretieren" bezeichnet. Die gängigsten Sprachen sind PCL (die am häufigsten auf HP-Druckern und ihren Klonen zum Einsatz kommt) und ESC/P (die bei Epson-Druckern verwendet wird). Diese Druckersprachen werden in der Regel von Linux unterstützt und liefern ein adäquates Druckergebnis. Linux ist unter Umständen nicht in der Lage, einige spezielle Druckerfunktionen anzusprechen. Mit Ausnahme der von HP entwickelten HPLIP (HP Linux Imaging & Printing) gibt es derzeit keinen Druckerhersteller, der Linux-Treiber entwickeln und sie den Linux-Distributoren unter einer Open-Source-Lizenz zur Verfügung stellen würde.

Proprietäre Drucker (auch GDI-Drucker genannt)
: Diese Drucker unterstützen keine der gängigen Druckersprachen. Sie verwenden eigene, undokumentierte Druckersprachen, die geändert werden können, wenn neue Versionen eines Modells auf den Markt gebracht werden. Für diese Drucker sind in der Regel nur Windows-Treiber verfügbar. Weitere Informationen finden Sie unter Abschnitt 15.7.1, „Drucker ohne Unterstützung für eine Standard-Druckersprache" (S. 215).

Vor dem Kauf eines neuen Druckers sollten Sie anhand der folgenden Quellen prüfen, wie gut der Drucker, den Sie zu kaufen beabsichtigen, unterstützt wird:

`http://www.linuxfoundation.org/OpenPrinting/`
: Die OpenPrinting-Homepage mit der Druckerdatenbank. In der Online-Datenbank wird der neueste Linux-Supportstatus angezeigt. Eine Linux-Distribution kann jedoch immer nur die zur Produktionszeit verfügbaren Treiber enthalten. Demnach ist es möglich, dass ein Drucker, der aktuell als „vollständig unterstützt" eingestuft wird, diesen Status bei der Veröffentlichung der neuesten SUSE Linux Enterprise Desktop-Version nicht aufgewiesen hat. Die Datenbank gibt daher nicht notwendigerweise den richtigen Status, sondern nur eine Annäherung an diesen an.

`http://pages.cs.wisc.edu/~ghost/`
: Die Ghostscript-Website

`/usr/share/doc/packages/ghostscript-library/catalog.devices`
: Liste inbegriffener Treiber.

15.1 Work-Flow des Drucksystems

Der Benutzer erstellt einen Druckauftrag. Der Druckauftrag besteht aus den zu druckenden Daten sowie aus Informationen für den Spooler, z. B. dem Namen des Druckers oder dem Namen der Druckwarteschlange und – optional – den Informationen für den Filter, z. B. druckerspezifische Optionen.

Mindestens eine zugeordnete Druckerwarteschlange ist für jeden Drucker vorhanden. Der Spooler hält den Druckauftrag in der Warteschlange, bis der gewünschte Drucker bereit ist, Daten zu empfangen. Wenn der Drucker druckbereit ist, sendet der Spooler die Daten über den Filter und das Backend an den Drucker.

Der Filter konvertiert die von der druckenden Anwendung generierten Daten (in der Regel PostScript oder PDF, aber auch ASCII, JPEG usw.) in druckerspezifische Daten (PostScript, PCL, ESC/P usw.). Die Funktionen des Druckers sind in den PPD-Dateien beschrieben. Eine PPD-Datei enthält druckspezifische Optionen mit den Parametern, die erforderlich sind, um die Optionen auf dem Drucker zu aktivieren. Das Filtersystem stellt sicher, dass die vom Benutzer ausgewählten Optionen aktiviert werden.

Wenn Sie einen PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten in druckerspezifische PostScript-Daten. Hierzu ist kein Druckertreiber erforderlich. Wenn Sie einen Nicht-PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten in druckerspezifische Daten. Hierzu ist ein für den Drucker geeigneter Druckertreiber erforderlich. Das Back-End empfängt die druckerspezifischen Daten vom Filter und leitet sie an den Drucker weiter.

15.2 Methoden und Protokolle zum Anschließen von Druckern

Es gibt mehrere Möglichkeiten, einen Drucker an das System anzuschließen. Die Konfiguration des CUPS-Drucksystems unterscheidet nicht zwischen einem lokalen Drucker und einem Drucker, der über das Netzwerk an das System angeschlossen ist.

WARNUNG: Ändern der Anschlüsse bei einem laufenden System

Vergessen Sie beim Anschließen des Druckers an den Computer nicht, dass während des Betriebs nur USB-Geräte angeschlossen werden können. Um Ihr System oder Ihren Drucker vor Schaden zu bewahren, fahren Sie das System herunter, wenn Sie Verbindungen ändern müssen, die keine USB-Verbindungen sind.

15.3 Installation der Software

PPD (PostScript Printer Description, PostScript-Druckerbeschreibung) ist die Computersprache, die die Eigenschaften, z. B. die Auflösung und Optionen wie die Verfügbarkeit einer Duplexeinheit, beschreibt. Diese Beschreibungen sind für die Verwendung der unterschiedlichen Druckeroptionen in CUPS erforderlich. Ohne eine PPD-Datei würden die Druckdaten in einem „rohen“ Zustand an den Drucker weitergeleitet werden, was in der Regel nicht erwünscht ist. Während der Installation von SUSE Linux Enterprise Desktop werden viele PPD-Dateien vorinstalliert.

Um einen PostScript-Drucker zu konfigurieren, sollten Sie sich zunächst eine geeignete PPD-Datei beschaffen. Viele PPD-Dateien sind im Paket `manufacturer-PPDs` enthalten, das im Rahmen der Standardinstallation automatisch installiert wird. Weitere Informationen hierzu finden Sie unter Abschnitt 15.6.2, „PPD-Dateien in unterschiedlichen Paketen“ (S. 213) und Abschnitt 15.7.2, „Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar“ (S. 216).

Neue PPD-Dateien können im Verzeichnis `/usr/share/cups/model/` gespeichert oder dem Drucksystem mit YaST hinzugefügt werden (siehe Abschnitt „Hinzufügen von Treibern mit YaST“ (Kapitel 5, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Bereitstellungshandbuch*)). Die PPD-Dateien lassen sich anschließend während der Druckereinrichtung auswählen.

Seien Sie vorsichtig, wenn Sie gleich ein ganzes Software-Paket eines Druckerherstellers installieren sollen. Diese Art der Installation würde erstens dazu führen, dass Sie die Unterstützung von SUSE Linux Enterprise Desktop verlieren, und zweitens können Druckbefehle anders funktionieren, und das System ist möglicherweise nicht mehr in der Lage, Geräte anderer Hersteller anzusprechen. Aus diesem Grund wird das Installieren von Herstellersoftware nicht empfohlen.

15.4 Netzwerkdrucker

Ein Netzwerkdrucker kann unterschiedliche Protokolle unterstützen - einige von diesen sogar gleichzeitig. Die meisten unterstützten Protokolle sind standardisiert, und doch versuchen einige Hersteller, diesen Standard abzuändern. Treiber werden meist nur für einige wenige Betriebsssysteme angeboten. Linux-Treiber werden leider nur sehr selten zur Verfügung gestellt. Gegenwärtig können Sie nicht davon ausgehen, dass alle Protokolle problemlos mit Linux funktionieren. Um dennoch eine funktionale Konfiguration zu erhalten, müssen Sie daher möglicherweise mit den verschiedenen Optionen experimentieren.

CUPS unterstützt die Protokolle `socket`, `LPD`, `IPP` und `smb`.

socket
: *Socket* bezeichnet eine Verbindung, über die die einfachen Druckdaten direkt an einen TCP-Socket gesendet werden. Einige der am häufigsten verwendeten Socket-Ports sind `9100` oder `35`. Die Syntax der Geräte-URI (Uniform Resource Identifier) lautet: socket://*`IP.für.den.Drucker`*:*`Port`*, beispielsweise: `socket://192.168.2.202:9100/`.

LPD (Line Printer Daemon)
: Das LDP-Protokoll wird in RFC 1179 beschrieben. Bei diesem Protokoll werden bestimmte auftragsspezifische Daten (z. B. die ID der Druckerwarteschlange) vor den eigentlichen Druckdaten gesendet. Beim Konfigurieren des LDP-Protokolls muss daher eine Druckerwarteschlange angegeben werden. Die Implementierungen diverser Druckerhersteller sind flexibel genug, um beliebige Namen als Druckwarteschlange zu akzeptieren. Der zu verwendende Name müsste ggf. im Druckerhandbuch angegeben sein. Es werden häufig Bezeichnungen wie LPT, LPT1, LP1 o. ä. verwendet. Die Portnummer für einen LPD-Dienst lautet `515`. Ein Beispiel für einen Gerät-URI ist `lpd://192.168.2.202/LPT1`.

IPP (Internet Printing Protocol)
: IPP ist ein relativ neues Protokoll (1999), das auf dem HTTP-Protokoll basiert. Mit IPP können mehr druckauftragsbezogene Daten übertragen werden als mit den anderen Protokollen. CUPS verwendet IPP für die interne Datenübertragung. Um IPP ordnungsgemäß konfigurieren zu können, ist der Name der Druckwarteschlange erforderlich. Die Portnummer für IPP lautet `631`. Beispiele für Geräte-URIs sind `ipp://192.168.2.202/ps` und `ipp://192.168.2.202/printers/ps`.

SMB (Windows-Freigabe)
: CUPS unterstützt auch das Drucken auf freigegebenen Druckern unter Windows. Das für diesen Zweck verwendete Protokoll ist SMB. SMB verwendet die Portnummern `137`, `138` und `139`. Beispiele für Geräte-URIs sind `smb://Benutzer:Passwort@Arbeitsgruppe/smb.example.com/Drucker`, `smb://Benutzer:Passwort@smb.example.com/Drucker` und `smb://smb.example.com/Drucker`.

Das vom Drucker unterstützte Protokoll muss vor der Konfiguration ermittelt werden. Wenn der Hersteller die erforderlichen Informationen nicht zur Verfügung stellt, können Sie das Protokoll mit dem Kommando `nmap` ermitteln, das Bestandteil des Pakets `nmap` ist. `nmap` überprüft einen Host auf offene Ports. Beispiel:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

15.4.1 Konfigurieren von CUPS mit Kommandozeilenwerkzeugen

CUPS kann mit Kommandozeilenwerkzeugen kofiguriert werden, beispielsweise `lpinfo`, `lpadmin` oder `lpoptions`. Sie benötigen ein Geräte-URI, das aus einem Backend, z. B. parallel, und Parametern besteht. Zum Bestimmen von gültigen Geräte-URIs auf Ihrem System verwenden Sie das Kommando `lpinfo -v | grep „:/“`:

```
# lpinfo -v | grep ":/"
direct usb://ACME/FunPrinter%20XL
direct parallel:/dev/lp0
```

Mit `lpadmin` kann der CUPS-Serveradministrator Druckerwarteschlangen hinzufügen, entfernen und verwalten. Verwenden Sie die folgende Syntax, um eine Druckwarteschlange hinzuzufügen:

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

Das Gerät (`-v`) ist anschließend als *`Warteschlange`* (`-p`) verfügbar und verwendet die angegebene PPD-Datei (`-P`). Das bedeutet, dass Sie die PPD-Datei und das Geräte-URI kennen müssen, wenn Sie den Drucker manuell konfigurieren möchten.

Verwenden Sie nicht `-E` als erste Option. Für alle CUPS-Befehle legt die Option `-E` als erstes Argument die Verwendung einer verschlüsselten Verbindung fest. Zur Akti-

vierung des Druckers muss die Option `-E` wie im folgenden Beispiel dargestellt verwendet werden:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

Im folgenden Beispiel wird ein Netzwerkdrucker konfiguriert:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Weitere Optionen von `lpadmin` finden Sie auf der man-Seiten von `lpadmin(8)`.

Während der Druckerkonfiguration werden bestimmte Optionen standardmäßig gesetzt. Diese Optionen können (je nach Druckwerkzeug) für jeden Druckauftrag geändert werden. Es ist auch möglich, diese Standardoptionen mit YaST zu ändern. Legen Sie die Standardoptionen mithilfe der Kommandozeilenwerkzeuge wie folgt fest:

1 Zeigen Sie zunächst alle Optionen an:

```
lpoptions -p queue -l
```

Beispiel:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

Die aktivierte Standardoption wird durch einen vorangestellten Stern (`*`) gekennzeichnet.

2 Ändern Sie die Option mit `lpadmin`:

```
lpadmin -p queue -o Resolution=600dpi
```

3 Prüfen Sie die neue Einstellung:

```
lpoptions -p queue -l

Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

Wenn ein normaler Benutzer `lpoptions` ausführt, werden die Einstellungen in `~/.cups/lpoptions` geschrieben. Jedoch werden die `root`-Einstellungen in to `/etc/cups/lpoptions` geschrieben.

15.5 Drucken über die Kommandozeile

Um den Druckvorgang über die Kommandozeile zu starten, geben Sie `lp -d` *`Name_der_WarteschlangeDateiname`* ein und ersetzen die entsprechenden Namen für *`Name_der_Warteschlange`* und *`Dateiname`*.

Einige Anwendungen erfordern für den Druckvorgang den Befehl `lp`. Geben Sie in diesem Fall den richtigen Befehl in das Druckdialogfeld der Anwendung ohne Angabe des *`Dateinamens`* ein, z. B. `lp -d` *`Name_der_Warteschlange`*.

15.6 Besondere Funktionen in SUSE Linux Enterprise Desktop

Für SUSE Linux Enterprise Desktop wurden mehrere CUPS-Funktionen angepasst. Im Folgenden werden einige der wichtigsten Änderungen beschrieben.

15.6.1 CUPS und Firewall

Nach einer Standardinstallation von SUSE Linux Enterprise Desktop ist SuSEFirewall2 aktiv, und die externen Netzwerkschnittstellen sind in der `externen Zone` konfiguriert, die eingehenden Datenverkehr blockiert. Weitere Informationen zur SUSEFirewall2-Konfiguration finden Sie in Section “SuSEfirewall2” (Chapter 15, *Masquerading and Firewalls*, ↑*Security Guide*) und unter `http://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings`.

15.6.1.1 CUPS-Client

Normalerweise wird der CUPS-Client auf einem normalen Arbeitsplatzrechner ausgeführt, die sich in einer verbürgten Netzwerkumgebung hinter einer Firewall befindet. In diesem Fall empfiehlt es sich, die Netzwerkschnittstelle in der `internen Zone` zu konfigurieren, damit der Arbeitsplatzrechner innerhalb des Netzwerks erreichbar ist.

15.6.1.2 CUPS-Server

Wenn der CUPS-Server Teil der durch eine Firewall geschützten verbürgten Netzwerkumgebung ist, sollte die Netzwerkschnittstelle in der `internen Zone` der Firewall konfiguriert sein. Es ist nicht empfehlenswert, einen CUPS-Server in einer nicht verbürgten Netzwerkumgebung einzurichten, es sei denn, Sie sorgen dafür, dass er durch besondere Firewall-Regeln und Sicherheitseinstellungen in der CUPS-Konfiguration geschützt wird.

15.6.2 PPD-Dateien in unterschiedlichen Paketen

Die YaST-Druckerkonfiguration richtet die Warteschlangen für CUPS auf dem System mit den in `/usr/share/cups/model/` installierten PPD-Dateien ein. Um die geeigneten PPD-Dateien für das Druckermodell zu finden, vergleicht YaST während der Hardware-Erkennung den Hersteller und das Modell mit den Herstellern und Modellen, die in den PPD-Dateien enthalten sind. Zu diesem Zweck generiert die YaST-Druckerkonfiguration eine Datenbank mit den Hersteller- und Modelldaten, die aus den PPD-Dateien extrahiert werden.

Die Konfiguration, die nur PPD-Dateien und keine weiteren Informationsquellen verwendet, hat den Vorteil, dass die PPD-Dateien in `/usr/share/cups/model/` beliebig geändert werden können. Wenn Sie beispielsweise nur mit PostScript-Druckern arbeiten, sind die Foomatic-PPD-Dateien im Paket `cups-drivers` oder die Gutenprint-PPD-Dateien im Paket `gutenprint` in der Regel nicht erforderlich. Stattdessen können die PPD-Dateien für die PostScript-Drucker direkt in `/usr/share/cups/model/` kopiert werden (wenn sie nicht bereits im Paket `manufacturer-PPDs` vorhanden sind), um eine optimale Konfiguration der Drucker zu erzielen.

15.6.2.1 CUPS-PPD-Dateien im Paket `cups`

Die generischen PPD-Dateien im Paket `cups` wurden durch angepasste Foomatic-PPD-Dateien für PostScript-Drucker der Level 1 und Level 2 ergänzt:

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

15.6.2.2 PPD-Dateien im Paket cups-drivers

Der Foomatic-Druckerfilter foomatic-rip wird in der Regel zusammen mit Ghostscript für Nicht-PostScript-Drucker verwendet. Geeignete Foomatic PPD-Dateien haben die Einträge *NickName: ... Foomatic/Ghostscript driver und *cupsFilter: ... foomatic-rip. Diese PPD-Dateien befinden sich im Paket cups-drivers.

YaST bevorzugt in der Regel eine Hersteller-PPD-Datei. Wenn jedoch keine passende Hersteller-PPD-Datei existiert, wird eine Foomatic-PPD-Datei mit dem Eintrag *Spitzname: ... Foomatic ... (empfohlen) ausgewählt.

15.6.2.3 Gutenprint-PPD-Dateien im gutenprint-Paket

Für viele Nicht-PostScript-Drucker kann anstelle von foomatic-rip der CUPS-Filter rastertogutenprint von Gutenprint (früher GIMP-Print) verwendet werden. Dieser Filter und die entsprechenden Gutenprint-PPD-Dateien befinden sich im Paket gutenprint. Die Gutenprint-PPD-Dateien befinden sich in /usr/share/cups/model/gutenprint/ und haben die Einträge *Spitzname: ... CUPS+Gutenprint und *cupsFilter: ... rastertogutenprint.

15.6.2.4 PPD-Dateien von Druckerherstellern im Paket manufacturer-PPDs

Das Paket manufacturer-PPDs enthält PPD-Dateien von Druckerherstellern, die unter einer ausreichend freien Lizenz veröffentlicht werden. PostScript-Drucker sollten mit der entsprechenden PPD-Datei des Druckerherstellers konfiguriert werden, da diese Datei die Verwendung aller Funktionen des PostScript-Druckers ermöglicht. YaST bevorzugt eine PPD-Datei aus den Hersteller-PPDs, kann jedoch keine PPD-Datei aus dem Paket der Hersteller-PPDs verwenden, wenn der Modellname nicht übereinstimmt. Dies kann geschehen, wenn das Paket der Hersteller-PPDs nur eine PPD-Datei für ähnliche Modelle enthält, z. B. Funprinter 12xx-Serie. Wählen Sie in diesem Fall die entsprechende PPD-Datei manuell in YaST aus.

15.7 Fehlersuche

In den folgenden Abschnitten werden einige der am häufigsten auftretenden Probleme mit der Druckerhardware und -software sowie deren Lösungen oder Umgehung beschrieben. Unter anderem werden die Themen GDI-Drucker, PPD-Dateien und Port-Konfiguration behandelt. Darüber hinaus werden gängige Probleme mit Netzwerkdruckern, fehlerhafte Ausdrucke und die Bearbeitung der Warteschlange erläutert.

15.7.1 Drucker ohne Unterstützung für eine Standard-Druckersprache

Diese Drucker unterstützen keine der geläufigen Druckersprachen und können nur mit proprietären Steuersequenzen adressiert werden. Daher funktionieren sie nur mit den Betriebssystemversionen, für die der Hersteller einen Treiber zur Verfügung stellt. GDI ist eine von Microsoft für Grafikgeräte entwickelte Programmierschnittstelle. In der Regel liefert der Hersteller nur Treiber für Windows, und da Windows-Treiber die GDI-Schnittstelle verwenden, werden diese Drucker auch *GDI-Drucker* genannt. Das eigentliche Problem ist nicht die Programmierschnittstelle, sondern die Tatsache, dass diese Drucker nur mit der proprietären Druckersprache des jeweiligen Druckermodells adressiert werden können.

Der Betrieb einiger GDI-Drucker kann sowohl im GDI-Modus als auch in einer der Standard-Druckersprachen ausgeführt werden. Sehen Sie im Druckerhandbuch nach, ob dies möglich ist. Einige Modelle benötigen für diese Umstellung eine spezielle Windows-Software. (Beachten Sie, dass der Windows-Druckertreiber den Drucker immer zurück in den GDI-Modus schalten kann, wenn von Windows aus gedruckt wird). Für andere GDI-Drucker sind Erweiterungsmodule für eine Standarddruckersprache erhältlich.

Einige Hersteller stellen für ihre Drucker proprietäre Treiber zur Verfügung. Der Nachteil proprietärer Druckertreiber ist, dass es keine Garantie gibt, dass diese mit dem installierten Drucksystem funktionieren oder für die unterschiedlichen Hardwareplattformen geeignet sind. Im Gegensatz dazu sind Drucker, die eine Standard-Druckersprache unterstützen, nicht abhängig von einer speziellen Drucksystemversion oder einer bestimmten Hardwareplattform.

Anstatt viel Zeit darauf aufzuwenden, einen herstellerspezifischen Linux-Treiber in Gang zu bringen, ist es unter Umständen kostengünstiger, einen Drucker zu erwerben, der eine Standarddruckersprache unterstützt (vorzugsweise PostScript). Dadurch wäre das Treiberproblem ein für alle Mal aus der Welt geschafft und es wäre nicht mehr erforderlich, spezielle Treibersoftware zu installieren und zu konfigurieren oder Treiber-Updates zu beschaffen, die aufgrund neuer Entwicklungen im Drucksystem benötigt würden.

15.7.2 Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar

Wenn das Paket `manufacturer-PPDs` für einen PostScript-Drucker keine geeignete PPD-Datei enthält, sollte es möglich sein, die PPD-Datei von der Treiber-CD des Druckerherstellers zu verwenden, oder eine geeignete PPD-Datei von der Webseite des Druckerherstellers herunterzuladen.

Wenn die PPD-Datei als Zip-Archiv (.zip) oder als selbstextrahierendes Zip-Archiv < ?dbsbr?>(.exe) zur Verfügung gestellt wird, entpacken Sie sie mit `unzip`. Lesen Sie zunächst die Lizenzvereinbarung für die PPD-Datei. Prüfen Sie dann mit dem Dienstprogramm `cupstestppd`, ob die PPD-Datei den Spezifikationen „Adobe PostScript Printer Description File Format Specification, Version 4.3.“ entspricht. Wenn das Dienstprogramm „FAIL“ zurückgibt, sind die Fehler in den PPD-Dateien schwerwiegend und werden sehr wahrscheinlich größere Probleme verursachen. Die von `cupstestppd` protokollierten Problempunkte müssen behoben werden. Fordern Sie beim Druckerhersteller ggf. eine geeignete PPD-Datei an.

15.7.3 Parallele Anschlüsse

Die sicherste Methode ist, den Drucker direkt an den ersten Parallelanschluss anzuschließen und im BIOS die folgenden Einstellungen für Parallelanschlüsse auszuwählen:

- E/A-Adresse: `378` (hexadezimal)
- Interrupt: nicht relevant
- Modus: `Normal`, `SPP` oder `Nur Ausgabe`

• DMA: deaktiviert

Wenn der Drucker trotz dieser Einstellungen über den Parallelanschluss nicht angesprochen werden kann, geben Sie die E/A-Adresse explizit entsprechend den Einstellungen im BIOS in der Form `0x378` in `/etc/modprobe.conf` ein. Wenn zwei Parallelanschlüsse vorhanden sind, die auf die E/A-Adressen `378` und `278` (hexadezimal) gesetzt sind, geben Sie diese in Form von `0x378,0x278` ein.

Wenn Interrupt `7` frei ist, kann er mit dem in Beispiel 15.1, „`/etc/modprobe.conf`: Interrupt-Modus für den ersten parallelen Port“ (S. 217) dargestellten Eintrag aktiviert werden. Prüfen Sie vor dem Aktivieren des Interrupt-Modus die Datei `/proc/interrupts`, um zu sehen, welche Interrupts bereits verwendet werden. Es werden nur die aktuell verwendeten Interrupts angezeigt. Dies kann sich je nachdem, welche Hardwarekomponenten aktiv sind, ändern. Der Interrupt für den Parallelanschluss darf von keinem anderen Gerät verwendet werden. Wenn Sie sich diesbezüglich nicht sicher sind, verwenden Sie den Polling-Modus mit `irq=none`.

Beispiel 15.1 * /etc/modprobe.conf: Interrupt-Modus für den ersten parallelen Port*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

15.7.4 Netzwerkdrucker-Verbindungen

Netzwerkprobleme identifizieren

Schließen Sie den Drucker direkt an den Computer an. Konfigurieren Sie den Drucker zu Testzwecken als lokalen Drucker. Wenn dies funktioniert, werden die Probleme netzwerkseitig verursacht.

TCP/IP-Netzwerk prüfen

Das TCP/IP-Netzwerk und die Namensauflösung müssen funktionieren.

Entfernten `lpd` prüfen

Geben Sie den folgenden Befehl ein, um zu testen, ob zu `lpd` (Port `515`) auf *`host`* eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 515 && echo ok || echo failed
```

Wenn die Verbindung zu `lpd` nicht hergestellt werden kann, ist `lpd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor.

Geben Sie als `root` den folgenden Befehl ein, um einen (möglicherweise sehr langen) Statusbericht für *`queue`* auf dem entfernten *`host`* abzufragen, vorausgesetzt, der entsprechende `lpd` ist aktiv und der Host akzeptiert Abfragen:

```
echo -e "\004queue" \
| netcat -w 2 -p 722 host 515
```

Wenn `lpd` nicht antwortet, ist er entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. Wenn `lpd` reagiert, sollte die Antwort zeigen, warum das Drucken in der `queue` auf `host` nicht möglich ist. Wenn Sie eine Antwort erhalten wie in Beispiel 15.2, „Fehlermeldung von `lpd`" (S. 218) gezeigt, wird das Problem durch den entfernten `lpd` verursacht.

***Beispiel 15.2** Fehlermeldung von lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Entfernten `cupsd` prüfen

Ein CUPS-Netzwerkserver kann die Warteschlangen standardmäßig alle 30 Sekunden per Broadcast über den UDP-Port `631` senden. Demzufolge kann mit dem folgenden Kommando getestet werden, ob im Netzwerk ein CUPS-Netzwerkserver mit aktivem Broadcast vorhanden ist. Stoppen Sie unbedingt Ihren lokalen CUPS-Daemon, bevor Sie das Kommando ausführen.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Wenn ein CUPS-Netzwerkserver vorhanden ist, der Informationen über Broadcasting sendet, erscheint die Ausgabe wie in Beispiel 15.3, „Broadcast vom CUPS-Netzwerkserver" (S. 218) dargestellt.

***Beispiel 15.3** Broadcast vom CUPS-Netzwerkserver*

```
ipp://192.168.2.202:631/printers/queue
```

Mit dem folgenden Befehl können Sie testen, ob mit `cupsd` (Port `631`) auf *`host`* eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 631 && echo ok || echo failed
```

Wenn die Verbindung zu `cupsd` nicht hergestellt werden kann, ist `cupsd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. `lpstat -h` *`host`* `-l -t` gibt einen (möglicherweise sehr langen) Statusbericht für alle

Warteschlangen auf *host* zurück, vorausgesetzt, dass der entsprechende `cupsd` aktiv ist und der Host Abfragen akzeptiert.

Mit dem nächsten Befehl können Sie testen, ob die *Warteschlange* auf *Host* einen Druckauftrag akzeptiert, der aus einem einzigen CR-Zeichen (Carriage-Return) besteht. In diesem Fall sollte nichts gedruckt werden. Möglicherweise wird eine leere Seite ausgegeben.

```
echo -en "\r" \
| lp -d queue -h host
```

Fehlerbehebung für einen Netzwerkdrucker oder eine Print Server Box

Spooler, die in einer Print Server Box ausgeführt werden, verursachen gelegentlich Probleme, wenn sie mehrere Druckaufträge bearbeiten müssen. Da dies durch den Spooler in der Print Server Box verursacht wird, gibt es keine Möglichkeit, dieses Problem zu beheben. Sie haben jedoch die Möglichkeit, den Spooler in der Print Server Box zu umgehen, indem Sie den an die Print Server Box angeschlossenen Drucker über den TCP-Socket direkt kontaktieren. Weitere Informationen hierzu finden Sie unter Abschnitt 15.4, „Netzwerkdrucker" (S. 209).

Auf diese Weise wird die Print Server-Box auf einen Konvertierer zwischen den unterschiedlichen Formen der Datenübertragung (TCP/IP-Netzwerk und lokale Druckerverbindung) reduziert. Um diese Methode verwenden zu können, müssen Sie den TCP-Port der Print Server Box kennen. Wenn der Drucker eingeschaltet und an die Print Server Box angeschlossen ist, kann dieser TCP-Port in der Regel mit dem Dienstprogramm `nmap` aus dem Paket `nmap` ermittelt werden, wenn die Print Server Box einige Zeit eingeschaltet ist. Beispiel: `nmap` *`IP-Adresse`* gibt die folgende Ausgabe für eine Print Server-Box zurück:

```
Port        State       Service
23/tcp      open        telnet
80/tcp      open        http
515/tcp     open        printer
631/tcp     open        cups
9100/tcp    open        jetdirect
```

Diese Ausgabe gibt an, dass der an die Print Server-Box angeschlossene Drucker über TCP-Socket an Port `9100` angesprochen werden kann. `nmap` prüft standardmäßig nur eine bestimmte Anzahl der allgemein bekannten Ports, die in `/usr/share/nmap/nmap-services` aufgeführt sind. Um alle möglichen Ports zu überprüfen, verwenden Sie den Befehl `nmap`

`-p` *`Ausgangs-Port-Ziel-PortIP-Adresse`*. Dies kann einige Zeit dauern. Weitere Informationen finden Sie auf der man-Seite zu `ypbind`.

Geben Sie einen Befehl ein wie

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

um Zeichenketten oder Dateien direkt an den entsprechenden Port zu senden, um zu testen, ob der Drucker auf diesem Port angesprochen werden kann.

15.7.5 Fehlerhafte Ausdrucke ohne Fehlermeldung

Für das Drucksystem ist der Druckauftrag abgeschlossen, wenn das CUPS-Back-End die Datenübertragung an den Empfänger (Drucker) abgeschlossen hat. Wenn die weitere Verarbeitung auf dem Empfänger nicht erfolgt (z. B. wenn der Drucker die druckerspezifischen Daten nicht drucken kann), wird dies vom Drucksystem nicht erkannt. Wenn der Drucker die druckerspezifischen Daten nicht drucken kann, wählen Sie eine PPD-Datei, die für den Drucker besser geeignet ist.

15.7.6 Deaktivierte Warteschlangen

Wenn die Datenübertragung zum Empfänger auch nach mehreren Versuchen nicht erfolgreich ist, meldet das CUPS-Back-End, z. B. `USB` oder `socket`, dem Drucksystem (an `cupsd`) einen Fehler. Das Backend bestimmt, wie viele erfolglose Versuche angemessen sind, bis die Datenübertragung als unmöglich gemeldet wird. Da weitere Versuche vergeblich wären, deaktiviert `cupsd` das Drucken für die entsprechende Warteschlange. Nachdem der Systemadministrator das Problem behoben hat, muss er das Drucken mit dem Kommando `cupsenable` wieder aktivieren.

15.7.7 CUPS-Browsing: Löschen von Druckaufträgen

Wenn ein CUPS-Netzwerkserver seine Warteschlangen den Client-Hosts via Browsing bekannt macht und auf den Host-Clients ein geeigneter lokaler `cupsd` aktiv ist,

akzeptiert der Client-`cupsd` Druckaufträge von Anwendungen und leitet sie an den `cupsd` auf dem Server weiter. Wenn `cupsd` auf dem Server einen Druckauftrag akzeptiert, wird diesem eine neue Auftragsnummer zugewiesen. Daher unterscheidet sich die Auftragsnummer auf dem Client-Host von der auf dem Server. Da ein Druckauftrag in der Regel sofort weitergeleitet wird, kann er mit der Auftragsnummer auf dem Client-Host nicht gelöscht werden. Dies liegt daran, dass der Client-`cupsd` den Druckauftrag als abgeschlossen betrachtet, sobald dieser an den Server-`cupsd` weitergeleitet wurde.

Wenn der Druckauftrag auf dem Server gelöscht werden soll, geben Sie ein Kommando wie `lpstat -h cups.example.com -o` ein. Sie ermitteln damit die Auftragsnummer auf dem Server, wenn der Server den Druckauftrag nicht bereits abgeschlossen (d. h. an den Drucker gesendet) hat. Mithilfe dieser Auftragsnummer kann der Druckauftrag auf dem Server gelöscht werden:

```
cancel -h cups.example.com queue-jobnumber
```

15.7.8 Fehlerhafte Druckaufträge und Fehler bei der Datenübertragung

Wenn Sie während des Druckvorgangs den Drucker oder den Computer abschalten, bleiben Druckaufträge in der Warteschlange. Der Druckvorgang wird wieder aufgenommen, sobald der Computer (bzw. der Drucker) wieder eingeschaltet wird. Fehlerhafte Druckaufträge müssen mit `cancel` aus der Warteschlange entfernt werden.

Wenn ein Druckauftrag fehlerhaft ist oder während der Kommunikation zwischen dem Host und dem Drucker ein Fehler auftritt, druckt der Drucker mehrere Seiten Papier mit unleserlichen Zeichen, da er die Daten nicht ordnungsgemäß verarbeiten kann. Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Um den Druckvorgang zu beenden, entfernen Sie das Papier aus Tintenstrahldruckern oder öffnen Sie die Papierzufuhr bei Laserdruckern. Qualitativ hochwertige Drucker sind mit einer Taste zum Abbrechen des aktuellen Druckauftrags ausgestattet.

2. Der Druckauftrag befindet sich möglicherweise noch in der Warteschlange, da die Aufträge erst dann entfernt werden, wenn sie vollständig an den Drucker übertragen wurden. Geben Sie `lpstat -o` oder `lpstat -h cups.example.com -o` ein, um zu prüfen, über welche Warteschlange aktuell gedruckt wird. Löschen Sie

den Druckauftrag mit `cancel` *`Warteschlange-Auftragsnummer`* oder `cancel -h cups.example.com` *`Warteschlange-Auftragsnummer`*.

3 Auch wenn der Druckauftrag aus der Warteschlange gelöscht wurde, werden einige Daten weiter an den Drucker gesendet. Prüfen Sie, ob ein CUPS-Backend-Prozess für die entsprechende Warteschlange ausgeführt wird und wenn ja, beenden Sie ihn. Für einen an den Parallelanschluss angeschlossenen Drucker geben Sie beispielsweise den Befehl `fuser -k /dev/lp0` ein, um alle Prozesse zu beenden, die aktuell noch auf den Drucker (den parallelen Port) zugreifen.

4 Setzen Sie den Drucker vollständig zurück, indem Sie ihn für einige Zeit ausschalten. Legen Sie anschließend Papier ein und schalten Sie den Drucker wieder ein.

15.7.9 Fehlerbehebung beim CUPS-Drucksystem

Suchen Sie Probleme im CUPS-Drucksystem mithilfe des folgenden generischen Verfahrens:

1 Setzen Sie `LogLevel debug` in `/etc/cups/cupsd.conf`.

2 Stoppen Sie `cupsd`.

3 Entfernen Sie `/var/log/cups/error_log*`, um das Durchsuchen sehr großer Protokolldateien zu vermeiden.

4 Starten Sie `cupsd`.

5 Wiederholen Sie die Aktion, die zu dem Problem geführt hat.

6 Lesen Sie die Meldungen in `/var/log/cups/error_log*`, um die Ursache des Problems zu identifizieren.

15.7.10 Weiterführende Informationen

Lösungen zu vielen spezifischen Problemen finden Sie in der SUSE Knowledgebase (http://www.suse.com/support/). Die relevanten Themen finden Sie am schnellsten mittels einer Textsuche nach CUPS.



Gerätemanagement über dynamischen Kernel mithilfe von udev

16

Der Kernel kann fast jedes Gerät in einem laufenden System hinzufügen oder entfernen. Änderungen des Gerätestatus (ob ein Gerät angeschlossen oder entfernt wird) müssen an den userspace weitergegeben werden. Geräte müssen konfiguriert werden, sobald sie angeschlossen und erkannt wurden. Die Benutzer eines bestimmten Geräts müssen über Änderungen im erkannten Status dieses Geräts informiert werden. udev bietet die erforderliche Infrastruktur, um die Geräteknotendateien und symbolischen Links im /dev-Verzeichnis dynamisch zu warten. udev–Regeln bieten eine Methode, um externe Werkzeuge an die Ereignisverarbeitung des Kernelgeräts anzuschließen. Auf diese Weise können Sie die udev-Gerätebehandlung anpassen. Beispielsweise, indem Sie bestimmte Skripten hinzufügen, die als Teil der Kernel-Gerätebehandlung ausgeführt werden, oder indem Sie zusätzliche Daten zur Auswertung bei der Gerätebehandlung anfordern und importieren.

16.1 Das /dev-Verzeichnis

Die Geräteknoten im /dev-Verzeichnis ermöglichen den Zugriff auf die entsprechenden Kernel-Geräte. Mithilfe von udev spiegelt das /dev-Verzeichnis den aktuellen Status des Kernels wieder. Jedes Kernel-Gerät verfügt über eine entsprechende Gerätedatei. Falls ein Gerät vom System getrennt wird, wird der Geräteknoten entfernt.

Der Inhalt des /dev-Verzeichnisses wird auf einem temporären Dateisystem gespeichert und alle Dateien werden bei jedem Systemstart gerendert. Manuell erstellte oder bearbeitete Dateien sind nicht dazu ausgelegt, einen Neustart zu überstehen. Statische

Dateien und Verzeichnisse, die unabhängig vom Status des entsprechenden Kernel-Geräts immer im /dev-Verzeichnis vorhanden sein sollten, können im Verzeichnis /lib/udev/devices platziert werden. Beim Systemstart wird der Inhalt des entsprechenden Verzeichnisses in das /dev-Verzeichnis kopiert und erhält dieselbe Eigentümerschaft und dieselben Berechtigungen wie die Dateien in /lib/udev/devices.

16.2 Kernel-uevents und udev

Die erforderlichen Geräteinformationen werden vom sysfs-Dateisystem exportiert. Für jedes Gerät, das der Kernel erkannt und initialisiert hat, wird ein Verzeichnis mit dem Gerätenamen erstellt. Es enthält Attributdateien mit gerätespezifischen Eigenschaften.

Jedes Mal, wenn ein Gerät hinzugefügt oder entfernt wird, sendet der Kernel ein uevent, um udev über die Änderung zu informieren. Der udev-Daemon liest und analysiert alle angegebenen Regeln aus den /etc/udev/rules.d/*.rules-Dateien einmalig beim Start und speichert diese. Wenn Regeldateien geändert, hinzugefügt oder entfernt werden, kann der Dämon die Arbeitsspeicherrepräsentation aller Regeln mithilfe des Kommandos udevadm control reload_rules wieder laden. Dies ist auch beim Ausführen von /etc/init.d/boot.udev reload möglich. Weitere Informationen zu den udev-Regeln und deren Syntax finden Sie unter Abschnitt 16.6, „Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von udev-Regeln“ (S. 230).

Jedes empfangene Ereignis wird mit dem Satz der angegebenen Regeln abgeglichen. Die Regeln können Ereignisergebnisschlüssel hinzufügen oder ändern, einen bestimmten Namen für den zu erstellenden Geräteknoten anfordern, auf den Knoten verweisende Symlinks hinzufügen oder Programme hinzufügen, die ausgeführt werden sollen, nachdem der Geräteknoten erstellt wurde. Die Treiber-Core-uevents werden von einem Kernel-Netlink-Socket empfangen.

16.3 Treiber, Kernel-Module und Geräte

Die Kernel-Bus-Treiber prüfen, ob Geräte vorhanden sind. Für jedes erkannte Gerät erstellt der Kernel eine interne Gerätestruktur, während der Treiber-Core ein uevent an den `udev`-Dämon sendet. Bus-Geräte identifizieren sich mithilfe einer speziell formatierten ID, die Auskunft über die Art des Geräts gibt. Normalerweise bestehen diese IDs aus einer Hersteller- und einer Produkt-ID und anderen das Subsystem betreffenden Werten. Jeder Bus weist ein eigenes Schema für diese IDs auf, das so genannte `MODALIAS`-Schema. Der Kernel bedient sich der Geräteinformationen, verfasst daraus eine `MODALIAS`-ID-Zeichenkette und sendet diese Zeichenkette zusammen mit dem Ereignis. Beispiel für eine USB-Maus:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Jeder Gerätetreiber verfügt über eine Liste bekannter Aliasse für Geräte, die er behandeln kann. Die Liste ist in der Kernel-Moduldatei selbst enthalten. Das Programm depmod liest die ID-Listen und erstellt die Datei `modules.alias` im Verzeichnis `/lib/modules` des Kernel für alle zurzeit verfügbaren Module. Bei dieser Infrastruktur ist das Laden des Moduls ein ebenso müheloser Vorgang, wie das Aufrufen von `modprobe` für jedes Ereignis, das über einen `MODALIAS`-Schlüssel verfügt. Falls `modprobe $MODALIAS` aufgerufen wird, gleicht es den für das Gerät verfassten Geräte-Alias mit den Aliassen von den Modulen ab. Falls ein übereinstimmender Eintrag gefunden wird, wird das entsprechende Modul geladen. Dies alles wird automatisch von `udev` ausgelöst.

16.4 Booten und erstes Einrichten des Geräts

Alle Geräteereignisse, die während des Bootvorgangs stattfinden, bevor der `udev`-Daemon ausgeführt wird, gehen verloren. Dies liegt daran, dass die Infrastruktur für die Behandlung dieser Ereignisse sich auf dem Root-Dateisystem befindet und zu diesem Zeitpunkt nicht verfügbar ist. Diesen Verlust fängt der Kernel mit der Datei `uevent` ab, die sich im Geräteverzeichnis jedes Geräts im sysfs-Dateisystem befindet. Durch das Schreiben von `add` in die entsprechende Datei sendet der Kernel dasselbe Ereignis, das während des Bootvorgangs verloren gegangen ist, neu. Eine einfache

Schleife über alle `uevent`-Dateien in `/sys` löst alle Ereignisse erneut aus, um die Geräteknoten zu erstellen und die Geräteeinrichtung durchzuführen.

Beispielsweise kann eine USB-Maus, die während des Bootvorgangs vorhanden ist, nicht durch die frühe Bootlogik initialisiert werden, da der Treiber zum entsprechenden Zeitpunkt nicht verfügbar ist. Das Ereignis für die Geräteerkennung ist verloren gegangen und konnte kein Kernel-Modul für das Gerät finden. Anstatt manuell nach möglicherweise angeschlossenen Geräten zu suchen, fordert `udev` lediglich alle Geräteereignisse aus dem Kernel an, wenn das Root-Dateisystem verfügbar ist. Das Ereignis für die USB-Maus wird also lediglich erneut ausgeführt. Jetzt wird das Kernel-Modul auf dem eingehängten Root-Dateisystem gefunden und die USB-Maus kann initialisiert werden.

Von userspace aus gibt es keinen erkennbaren Unterschied zwischen einer coldplug-Gerätesequenz und einer Geräteerkennung während der Laufzeit. In beiden Fällen werden dieselben Regeln für den Abgleich verwendet und dieselben konfigurierten Programme ausgeführt.

16.5 Überwachen des aktiven `udev`-Daemons

Das Programm `udevadm monitor` kann verwendet werden, um die Treiber-Core-Ereignisse und das Timing der udev-Ereignisprozesse zu visualisieren.

```
UEVENT[1185238505.276660] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV  [1185238505.279198] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV  [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV  [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
```

```
UDEV  [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

Die `UEVENT`-Zeilen zeigen die Ereignisse an, die der Kernel an Netlink gesendet hat. Die `UDEV`-Zeilen zeigen die fertig gestellten udev-Ereignisbehandlungsroutinen an. Das Timing wird in Mikrosekunden angegeben. Die Zeit zwischen `UEVENT` und `UDEV` ist die Zeit, die udev benötigt hat, um dieses Ereignis zu verarbeiten oder der udev-Daemon hat eine Verzögerung bei der Ausführung der Synchronisierung dieses Ereignisses mit zugehörigen und bereits ausgeführten Ereignissen erfahren. Beispielsweise warten Ereignisse für Festplattenpartitionen immer, bis das Ereignis für den primären Datenträger fertig gestellt ist, da die Partitionsereignisse möglicherweise auf die Daten angewiesen sind, die das Ereignis für den primären Datenträger von der Hardware angefordert hat.

`udevadm monitor --env` zeigt die vollständige Ereignisumgebung an:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

`udev sendet auch Meldungen an syslog.` Die Standard-syslog-Priorität, die steuert, welche Meldungen an syslog gesendet werden, wird in der `udev`-Konfigurationsdatei `/etc/udev/udev.conf` angegeben. Die Protokollpriorität des ausgeführten Dämons kann mit `udevadm control log_priority=`*`level/number`* geändert werden.

16.6 Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von udev-Regeln

Eine udev-Regel kann mit einer beliebigen Eigenschaft abgeglichen werden, die der Kernel der Ereignisliste hinzufügt oder mit beliebigen Informationen, die der Kernel in sysfs exportiert. Die Regel kann auch zusätzliche Informationen aus externen Programmen anfordern. Jedes Ereignis wird gegen alle angegebenen Regeln abgeglichen. Alle Regeln befinden sich im Verzeichnis /etc/udev/rules.d/.

Jede Zeile in der Regeldatei enthält mindestens ein Schlüsselwertepaar. Es gibt zwei Arten von Schlüsseln: die Übereinstimmungsschlüssel und Zuweisungsschlüssel. Wenn alle Übereinstimmungsschlüssel mit ihren Werten übereinstimmen, wird diese Regel angewendet und der angegebene Wert wird den Zuweisungsschlüsseln zugewiesen. Eine übereinstimmende Regel kann den Namen des Geräteknotens angeben, auf den Knoten verweisende Symlinks hinzufügen oder ein bestimmtes Programm als Teil der Ereignisbehandlung ausführen. Falls keine übereinstimmende Regel gefunden wird, wird der standardmäßige Geräteknotenname verwendet, um den Geräteknoten zu erstellen. Ausführliche Informationen zur Regelsyntax und den bereitgestellten Schlüsseln zum Abgleichen oder Importieren von Daten werden auf der man-Seite von udev beschrieben. Nachfolgend finden Sie einige Beispielregeln, die Sie in die grundlegende Regelsyntax von udev einführen. Sämtliche Beispielregeln stammen aus dem udev-Standardregelsatz, der sich in /etc/udev/rules.d/50-udev -default.rules befindet.

***Beispiel 16.1** udev-Beispielregeln*

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

Die Regel Konsole besteht aus drei Schlüsseln: einem Übereinstimmungsschlüssel (KERNEL) und zwei Zuweisungsschlüsseln (MODE, OPTIONS). Der Übereinstimmungsschlüssel KERNEL durchsucht die Geräteliste nach Elementen des Typs console. Nur exakte Übereinstimmungen sind gültig und lösen die Ausführung dieser Regel aus. Der Zuweisungsschlüssel MODE weist dem Geräteknoten spezielle Berechtigungen zu, in diesem Fall Lese- und Schreibberechtigung nur für den Eigentümer des Geräts. Der Schlüssel OPTIONS bewirkt, dass diese Regel auf Geräte dieses Typs als letzte Regel angewendet wird. Alle nachfolgenden Regeln, die mit diesem Gerätetyp übereinstimmen, werden nicht mehr angewendet.

Die Regel serial devices steht in 50-udev-default.rules nicht mehr zur Verfügung; es lohnt sich jedoch, sie sich dennoch anzusehen. Sie besteht aus zwei Übereinstimmungsschlüsseln (KERNEL und ATTRS) und einem Zuweisungsschlüssel (SYMLINK). Der Übereinstimmungsschlüssel KERNEL sucht nach allen Geräten des Typs ttyUSB. Durch den Platzhalter * trifft dieser Schlüssel auf mehrere dieser Geräte zu. Der zweite Übereinstimmungsschlüssel (ATTRS) überprüft, ob die Attributdatei product in sysfs der jeweiligen ttyUSB-Geräte eine bestimmte Zeichenkette enthält. Der Zuweisungsschlüssel SYMLINK bewirkt, dass dem Gerät unter /dev/pilot ein symbolischer Link hinzugefügt wird. Der Operator dieses Schlüssels (+=) weist udev an, diese Aktion auch dann auszuführen, wenn dem Gerät bereits durch frühere (oder auch erst durch spätere) Regeln andere symbolische Links hinzugefügt wurden. Die Regel wird nur angewendet, wenn die Bedingungen beider Übereinstimmungsschlüssel erfüllt sind.

Die Regel printer gilt nur für USB-Drucker. Sie enthält zwei Übereinstimmungsschlüssel (SUBSYSTEM und KERNEL), die beide zutreffen müssen, damit die Regel angewendet wird. Die drei Zuweisungsschlüssel legen den Namen dieses Gerätetyps fest (NAME), die Erstellung symbolischer Gerätelinks (SYMLINK) sowie die Gruppenmitgliedschaft dieses Gerätetyps (GROUP). Durch den Platzhalter * im Schlüssel KERNEL trifft diese Regel auf mehrere lp-Druckergeräte zu. Sowohl der Schlüssel NAME als auch der Schlüssel SYMLINK verwenden Ersetzungen, durch die der Zeichenkette der interne Gerätename hinzugefügt wird. Der symbolische Link für den ersten lp-USB-Drucker würde zum Beispiel /dev/usblp0 lauten.

Die Regel kernel firmware loader weist udev an, während der Laufzeit weitere Firmware mittels eines externen Hilfsskripts zu laden. Der Übereinstimmungsschlüssel SUBSYSTEM sucht nach dem Subsystem firmware. Der Schlüssel ACTION überprüft, ob bereits Geräte des Subsystems firmware hinzugefügt wurden. Der

Schlüssel RUN+= löst die Ausführung des Skripts firmware.sh aus, das die noch zu ladende Firmware lokalisiert.

Die folgenden allgemeinen Eigenschaften treffen auf alle Regeln zu:

- Jede Regel besteht aus einem oder mehreren, durch Kommas getrennten Schlüssel-/Wertepaaren.
- Die Aktion eines Schlüssels wird durch seinen Operator festgelegt. udev-Regeln unterstützen verschiedene Operatoren.
- Jeder angegebene Wert muss in Anführungszeichen eingeschlossen sein.
- Jede Zeile der Regeldatei stellt eine Regel dar. Falls eine Regel länger als eine Zeile ist, verbinden Sie die Zeilen wie bei jeder anderen Shell-Syntax mit \.
- udev-Regeln unterstützen Shell-typische Übereinstimmungsregeln für die Schemata *, ? und [].
- udev-Regeln unterstützen Ersetzungen.

16.6.1 Verwenden von Operatoren in udev-Regeln

Bei der Erstellung von Schlüsseln stehen Ihnen je nach gewünschtem Schlüsseltyp verschiedene Operatoren zur Auswahl. Übereinstimmungsschlüssel werden in der Regel nur zum Auffinden eines Wertes verwendet, der entweder mit dem Suchwert übereinstimmt oder explizit nicht mit dem gesuchten Wert übereinstimmt. Übereinstimmungsschlüssel enthalten einen der folgenden Operatoren:

==

Suche nach übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

!=

Suche nach nicht übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

Folgende Operatoren können für Zuweisungsschlüssel verwendet werden:

=
: Weist einem Schlüssel einen Wert zu. Wenn der Schlüssel zuvor aus einer Liste mit mehreren Werten bestand, wird der Schlüssel durch diesen Operator auf diesen Einzelwert zurückgesetzt.

+=
: Fügt einem Schlüssel, der eine Liste mehrerer Einträge enthält, einen Wert hinzu.

:=
: Weist einen endgültigen Wert zu. Eine spätere Änderung durch nachfolgende Regeln ist nicht möglich.

16.6.2 Verwenden von Ersetzungen in udev-Regeln

`udev`–Regeln unterstützen sowohl Platzhalter als auch Ersetzungen. Diese setzen Sie genauso ein wie in anderen Skripten. Folgende Ersetzungen können in `udev`-Regeln verwendet werden:

`%r`, `$root`
: Standardmäßig das Geräteverzeichnis `/dev`.

`%p`, `$devpath`
: Der Wert von `DEVPATH`.

`%k`, `$kernel`
: Der Wert von `KERNEL` oder der interne Gerätename.

`%n`, `$number`
: Die Gerätenummer.

`%N`, `$tempnode`
: Der temporäre Name der Gerätedatei.

`%M`, `$major`
: Die höchste Nummer des Geräts.

`%m`, `$minor`
: Die niedrigste Nummer des Geräts.

`%s{`*`attribute`*`}`, `$attr{`*`attribute`*`}`
: Der Wert eines `sysfs`-Attributs (das durch *`attribute`* festgelegt ist).

`%E{`*`variable`*`}`, `$attr{`*`variable`*`}`
: Der Wert einer Umgebungsvariablen (die durch *`variable`* festgelegt ist).

`%c`, `$result`
: Die Ausgabe von `PROGRAM`.

`%%`
: Das `%`-Zeichen.

`$$`
: Das `$`-Zeichen.

16.6.3 Verwenden von `udev`-Übereinstimmungsschlüsseln

Übereinstimmungsschlüssel legen Bedingungen fest, die erfüllt sein müssen, damit eine `udev`-Regel angewendet werden kann. Folgende Übereinstimmungsschlüssel sind verfügbar:

`ACTION`
: Der Name der Ereignisaktion, z. B. `add` oder `remove` beim Hinzufügen oder Entfernen eines Geräts.

`DEVPATH`
: Der Gerätepfad des Ereignisgeräts, zum Beispiel `DEVPATH=/bus/pci/drivers/ipw3945` für die Suche nach allen Ereignissen in Zusammenhang mit dem Treiber ipw3945.

`KERNEL`
: Der interne Name (Kernel-Name) des Ereignisgeräts.

`SUBSYSTEM`
: Das Subsystem des Ereignisgeräts, zum Beispiel `SUBSYSTEM=usb` für alle Ereignisse in Zusammenhang mit USB-Geräten.

`ATTR{`*`Dateiname`*`}`
: `sysfs-Attribute des Ereignisgeräts.` Für die Suche nach einer Zeichenkette im Attributdateinamen `vendor` können Sie beispielsweise `ATTR{vendor}==„On[sS]tream“` verwenden.

`KERNELS`
: Weist `udev` an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätenamen zu durchsuchen.

`SUBSYSTEMS`
: Weist `udev` an, den Gerätepfad aufwärts nach einem übereinstimmenden Geräte-Subsystemnamen zu durchsuchen.

`DRIVERS`
: Weist `udev` an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätetreibernamen zu durchsuchen.

`ATTRS{`*`Dateiname`*`}`
: Weist `udev` an, den Gerätepfad aufwärts nach einem Gerät mit übereinstimmenden `sysfs`-Attributwerten zu durchsuchen.

`ENV{`*`Schlüssel`*`}`
: Der Wert einer Umgebungsvariablen, zum Beispiel `ENV{ID_BUS}=„ieee1394` für die Suche nach allen Ereignissen in Zusammenhang mit der FireWire-Bus-ID.

`PROGRAM`
: Weist `udev` an, ein externes Programm auszuführen. Damit es erfolgreich ist, muss das Programm mit Beendigungscode Null abschließen. Die Programmausgabe wird in stdout geschrieben und steht dem Schlüssel `RESULT` zur Verfügung.

`RESULT`
: Überprüft die Rückgabezeichenkette des letzten `PROGRAM`-Aufrufs. Diesen Schlüssel können Sie entweder sofort der Regel mit dem `PROGRAM`-Schlüssel hinzufügen oder erst einer nachfolgenden Regel.

16.6.4 Verwenden von udev-Zuweisungsschlüsseln

Im Gegensatz zu den oben beschriebenen Übereinstimmungsschlüsseln beschreiben Zuweisungsschlüssel keine Bedingungen, die erfüllt werden müssen. Sie weisen den Geräteknoten, die von `udev` gewartet werden, Werte, Namen und Aktionen zu.

`NAME`
: Der Name des zu erstellenden Geräteknotens. Nachdem der Knotenname durch eine Regel festgelegt wurde, werden alle anderen Regeln mit dem Schlüssel `NAME`, die auf diesen Knoten zutreffen, ignoriert.

`SYMLINK`
: Der Name eines symbolischen Links, der dem zu erstellenden Knoten hinzugefügt werden soll. Einem Geräteknoten können mittels mehrerer Zuweisungsregeln mehrere symbolische Links hinzugefügt werden. Ebenso können Sie aber mehrere symbolische Links für einen Knoten auch in einer Regel angeben. Die Namen der einzelnen Symlinks müssen in diesem Fall jeweils durch ein Leerzeichen getrennt sein.

`OWNER, GROUP, MODE`
: Die Berechtigungen für den neuen Geräteknoten. Die hier angegebenen Werte überschreiben sämtliche kompilierten Werte.

`ATTR{`*`Schlüssel`*`}`
: Gibt einen Wert an, der in ein `sysfs`-Attribut des Ereignisgeräts geschrieben werden soll. Wenn der Operator == verwendet wird, überprüft dieser Schlüssel, ob der Wert eines sysfs-Attributs mit dem angegebenen Wert übereinstimmt.

`ENV{`*`Schlüssel`*`}`
: Weist `udev` an, eine Umgebungsvariable zu exportieren. Wenn der Operator == verwendet wird, überprüft dieser Schlüssel, ob der Wert einer Umgebungsvariable mit dem angegebenen Wert übereinstimmt.

`RUN`
: Weist `udev` an, der Liste der für dieses Gerät auszuführenden Programme ein Programm hinzuzufügen. Sie sollten hier nur sehr kurze Aufgaben angeben.

Anderenfalls laufen Sie Gefahr, dass weitere Ereignisse für dieses Gerät blockiert werden.

`LABEL`
: Fügt der Regel eine Bezeichnung hinzu, zu der ein `GOTO` direkt wechseln kann.

`GOTO`
: Weist `udev` an, eine Reihe von Regeln auszulassen und direkt mit der Regel fortzufahren, die die von `GOTO` angegebene Bezeichnung enthält.

`IMPORT{`*`Typ`*`}`
: Lädt Variablen in die Ereignisumgebung, beispielsweise die Ausgabe eines externen Programms. `udev` kann verschiedene Variablentypen importieren. Wenn kein Typ angegeben ist, versucht `udev` den Typ anhand des ausführbaren Teils der Dateiberechtigungen selbst zu ermitteln.

- `program` weist `udev` an, ein externes Programm auszuführen und dessen Ausgabe zu importieren.
- `file` weist `udev` an, eine Textdatei zu importieren.
- `parent` weist `udev` an, die gespeicherten Schlüssel des übergeordneten Geräts zu importieren.

`WAIT_FOR_SYSFS`
: Weist `udev` an, auf die Erstellung der angegebenen `sysfs`-Datei für ein bestimmtes Gerät zu warten. Beispiel: `WAIT_FOR_SYSFS=„ioerr_cnt“` fordert `udev` auf, so lange zu warten, bis die Datei `ioerr_cnt` erstellt wurde.

`OPTIONEN`
: Der Schlüssel `OPTION` kann mehrere mögliche Werte haben:

- `last_rule` weist `udev` an, alle nachfolgenden Regeln zu ignorieren.
- `ignore_device` weist `udev` an, dieses Ereignis komplett zu ignorieren.
- `ignore_remove` weist `udev` an, alle späteren Entfernungsereignisse für dieses Gerät zu ignorieren.

- `all_partitions` weist `udev` an, für alle vorhandenen Partitionen eines Blockgeräts Geräteknoten zu erstellen.

16.7 Permanente Gerätebenennung

Das dynamische Geräteverzeichnis und die Infrastruktur für die `udev`-Regeln ermöglichen die Bereitstellung von stabilen Namen für alle Laufwerke unabhängig von ihrer Erkennungsreihenfolge oder der für das Gerät verwendeten Verbindung. Jedes geeignete Blockgerät, das der Kernel erstellt, wird von Werkzeugen mit speziellen Kenntnissen über bestimmte Busse, Laufwerktypen oder Dateisysteme untersucht. Gemeinsam mit dem vom dynamischen Kernel bereitgestellten Geräteknotennamen unterhält `udev` Klassen permanenter symbolischer Links, die auf das Gerät verweisen:

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

16.8 Von udev verwendete Dateien

/sys/*
: Virtuelles, vom Linux-Kernel bereitgestelltes Dateisystem, das alle zur Zeit bekannten Geräte exportiert. Diese Informationen werden von udev zur Erstellung von Geräteknoten in /dev verwendet.

/dev/*
: Dynamisch erstellte Geräteknoten und statische Inhalte, die beim Booten aus /lib/udev/devices/* kopiert werden.

Die folgenden Dateien und Verzeichnisse enthalten die entscheidenden Elemente der udev-Infrastruktur:

/etc/udev/udev.conf
: Wichtigste udev-Konfigurationsdatei.

/etc/udev/rules.d/*
: udev-Ereigniszuordnungsregeln.

/lib/udev/devices/*
: Statischer /dev-Inhalt.

/lib/udev/*
: Von den udev-Regeln aufgerufene Helferprogramme.

16.9 Weiterführende Informationen

Weitere Informationen zur udev-Infrastruktur finden Sie auf den folgenden Manualpages:

udev
: Allgemeine Informationen zu udev, Schlüsseln, Regeln und anderen wichtigen Konfigurationsbelangen.

`udevadm`
: `udevadm` kann dazu verwendet werden, das Laufzeitverhalten von `udev` zu kontrollieren, Kernel-Ereignisse abzurufen, die Ereigniswarteschlange zu verwalten und einfache Methoden zur Fehlersuche bereitzustellen.

`udevd`
: Informationen zum `udev`-Ereignisverwaltungs-Daemon.

Das X Window-System 17

Das X Window-System (X11) ist der Industriestandard für grafische Bedienoberflächen unter UNIX. X ist netzwerkbasiert und ermöglicht es, auf einem Host gestartete Anwendungen auf einem anderen, über eine beliebige Art von Netzwerk (LAN oder Internet) verbundenen Host anzuzeigen. In diesem Kapitel werden die Einrichtung und die Optimierung der X Window-Systemumgebung beschrieben. Sie erhalten dabei Hintergrundinformationen zur Verwendung von Schriften in SUSE® Linux Enterprise Desktop.

17.1 Manuelles Konfigurieren des X Window-Systems

Standardmäßig ist das X Window System mit der unter Abschnitt „Einrichten von Grafikkarte und Monitor“ (Kapitel 5, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Bereitstellungshandbuch*) beschriebenen SaX2-Schnittstelle konfiguriert. Alternativ kann er manuell konfiguriert werden, indem Sie die entsprechenden Konfigurationsdateien bearbeiten.

WARNUNG: Fehlerhafte X-Konfigurationen können Ihre Hardware beschädigen

Seien Sie sehr vorsichtig, wenn Sie die Konfiguration des X Window-Systems ändern. Starten Sie auf keinen Fall das X Window-System, bevor die Konfiguration abgeschlossen ist. Ein falsch konfiguriertes System kann Ihre Hardware irreparabel beschädigen (dies gilt insbesondere für Monitore mit fester Fre-

quenz). Die Autoren dieses Buchs und die Entwickler von SUSE Linux Enterprise Desktop übernehmen keine Haftung für mögliche Schäden. Die folgenden Informationen basieren auf sorgfältiger Recherche. Es kann jedoch nicht garantiert werden, dass alle hier aufgeführten Methoden fehlerfrei sind und keinen Schaden an Ihrer Hardware verursachen können.

Das Kommando `sax2` erstellt die Datei `/etc/X11/xorg.conf`. Dabei handelt es sich um die primäre Konfigurationsdatei des X Window System. Hier finden Sie alle Einstellungen, die Grafikkarte, Maus und Monitor betreffen.

WICHTIG: Verwenden von X -configure

Konfigurieren Sie Ihr X-Setup mit `X -configure`, wenn vorherige Versuche mit SaX2 von SUSE Linux Enterprise Desktop nicht erfolgreich waren. Wenn Ihre Einrichtung proprietäre ausschließlich binäre Treiber umfasst, funktioniert `X -configure` nicht.

In den folgenden Abschnitten wird die Struktur der Konfigurationsdatei `/etc/X11/xorg.conf` beschrieben. Sie ist in mehrere Abschnitte gegliedert, die jeweils für bestimmte Aspekte der Konfiguration verantwortlich sind. Jeder Abschnitt beginnt mit dem Schlüsselwort `Section <Bezeichnung>` und endet mit `EndSection`. Die folgende Konvention gilt für alle Abschnitte:

```
Section "designation"
  entry 1
  entry 2
  entry n
EndSection
```

Die verfügbaren Abschnittstypen finden Sie in Tabelle 17.1, „Abschnitte in /etc/X11/xorg.conf“ (S. 242).

***Tabelle 17.1** Abschnitte in /etc/X11/xorg.conf*

Typ	Bedeutung
`Dateien`	Die Pfade für die Schriften und die RGB-Farbtabelle.
`ServerFlags`	Allgemeine Schalter für das Serververhalten.

Typ	Bedeutung
`Modul`	Eine Liste mit Modulen, die der Server laden sollte
`InputDevice`	Eingabegeräte wie Tastaturen und spezielle Eingabegeräte (Touchpads, Joysticks usw.) werden in diesem Abschnitt konfiguriert. Wichtige Parameter in diesem Abschnitt sind `Driver` und die Optionen für `Protocol` und `Device`. Normalerweise ist dem Computer ein `InputDevice`-Abschnitt pro Gerät angefügt.
`Monitor`	Der verwendete Monitor. Wichtige Elemente dieses Abschnitts sind die Kennung (`Identifier`), auf die später in der Definition von `Screen` eingegangen wird, die Aktualisierungsrate (`VertRefresh`) und die Grenzwerte für die Synchronisierungsfrequenz (`HorizSync` und `VertRefresh`). Die Einstellungen sind in MHz, kHz und Hz angegeben. Normalerweise akzeptiert der Server nur Modeline-Werte, die den Spezifikationen des Monitors entsprechen. Dies verhindert, dass der Monitor versehentlich mit zu hohen Frequenzen angesteuert wird.
`Modi`	Die Modeline-Parameter für die spezifischen Bildschirmauflösungen. Diese Paramter können von SaX2 auf Grundlage der vom Benutzer vorgegebenen Werte berechnet werden und

Typ	Bedeutung
	müssen in der Regel nicht geändert werden. Nehmen Sie hier beispielsweise dann Änderungen vor, wenn Sie einen Monitor mit fester Frequenz anschließen möchten. Details zur Bedeutung der einzelnen Zahlenwerte finden Sie in den HOWTO-Dateien unter `/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO` (im Paket `howtoenh`). Zur manuellen Berechnung von VESA-Modi können Sie das Tool `cvt` verwenden. Verwenden Sie z. B. zur Berechnung einer Modeline für einen 1680x1050@60Hz-Monitor das Kommando `cvt 1680 1050 60`.
`Gerät`	Eine spezifische Grafikkarte. Sie wird mit ihrem beschreibenden Namen angeführt. Die in diesem Abschnitt verfügbaren Optionen hängen stark vom verwendeten Treiber ab. Wenn Sie beispielsweise den `i810`-Treiber verwenden, erhalten Sie weitere Informationen auf der man-Seite `man 4 i810`.
`Screen`	Hier wird eine Verbindung zwischen einem `Monitor` und einer Grafikkarte (`Device`) hergestellt, wodurch alle erforderlichen Einstellungen für X.Org bereitgestellt werden. Im Unterabschnitt `Display` können Sie die Größe des virtuellen Bildschirms

Typ	Bedeutung
	(Virtual), den ViewPort und die Modes für diesen Bildschirm festlegen. Beachten Sie, dass einige Treiber es erfordern, dass alle verwendeten Konfigurationen an einer Stelle im Abschnitt Display vorhanden sein müssen. Wenn Sie beispielsweise an einem Laptop einen externen Monitor verwenden möchten, der größer als das interne LCD-Display ist, kann es erforderlich sein, eine höhere Auflösung als die vom internen LCD-Display unterstützte an das Ende der Zeile Modes anzufügen.
ServerLayout	Das Layout einer Einzel- oder Multihead-Konfiguration. In diesem Abschnitt werden Kombinationen aus Eingabegeräten (InputDevice) und Anzeigegeräten (Screen) festgelegt.
DRI	Bietet Informationen für die Direct Rendering Infrastructure (DRI).

Monitor, Device und Screen werden genauer erläutert. Weitere Informationen zu den anderen Abschnitten finden Sie auf den Manualpages von X.Org und xorg.conf.

Die Datei xorg.conf kann mehrere unterschiedliche Abschnitte vom Typ Monitor und Device enthalten. Manchmal gibt es sogar mehrere Abschnitte vom Typ Screen. Der Abschnitt ServerLayout legt fest, welche dieser Abschnitte verwendet werden.

17.1.1 Abschnitt „Screen“

Der Abschnitt „Screen“ kombiniert einen Monitor mit einem Device-Abschnitt und legt fest, welche Auflösung und Farbtiefe verwendet werden sollen. Der Abschnitt „Screen“ kann beispielsweise wie in Beispiel 17.1, „Abschnitt „Screen“ der Datei /etc/X11/xorg.conf“ (S. 246) aussehen.

***Beispiel 17.1** Abschnitt „Screen“ der Datei /etc/X11/xorg.conf*

```
Section "Screen"❶
  DefaultDepth  16❷
  SubSection "Display"❸
    Depth       16❹
    Modes       "1152x864" "1024x768" "800x600"❺
    Virtual     1152x864❻
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"❼
  Monitor       "Monitor[0]"
EndSection
```

❶ `Section` legt den Typ des Abschnitts fest, in diesem Fall `Screen`.

❷ `DefaultDepth` bestimmt die Farbtiefe, die standardmäßig verwendet werden soll, wenn keine andere Farbtiefe explizit angegeben wird.

❸ Für jede Farbtiefe werden verschiedene `Display`-Unterabschnitte angegeben.

❹ `Depth` bestimmt die Farbtiefe, die mit diesem Satz von `Display`-Einstellungen benutzt werden soll. Mögliche Werte sind `8`, `15`, `16`, `24` und `32`, obwohl möglicherweise nicht alle davon durch alle X-Server-Module oder -Auflösungen unterstützt werden.

❺ Der Abschnitt `Modes` enthält eine Liste der möglichen Bildschirmauflösungen. Diese Liste wird vom X-Server von links nach rechts gelesen. Zu jeder Auflösung sucht der X-Server eine passende `Modeline` im Abschnitt `Modes`. Die

Modeline ist von den Fähigkeiten des Monitors und der Grafikkarte abhängig. Die Einstellungen unter Monitor bestimmen die Modeline.

Die erste passende Auflösung ist der Standardmodus (Default mode). Mit Strg + Alt + + (auf dem Ziffernblock) können Sie zur nächsten Auflösung rechts in der Liste wechseln. Mit Strg + Alt + – (auf dem Ziffernblock) können Sie zur vorherigen Auflösung wechseln. So lässt sich die Auflösung ändern, während X ausgeführt wird.

❻ Die letzte Zeile des Unterabschnitts Display mit Depth 16 bezieht sich auf die Größe des virtuellen Bildschirms. Die maximal mögliche Größe eines virtuellen Bildschirms ist von der Menge des Arbeitsspeichers auf der Grafikkarte und der gewünschten Farbtiefe abhängig, nicht jedoch von der maximalen Auflösung des Monitors. Wenn Sie diese Zeile auslassen, entspricht die virtuelle Auflösung der physikalischen Auflösung. Da moderne Grafikkarten über viel Grafikspeicher verfügen, können Sie sehr große virtuelle Desktops erstellen. Gegebenenfalls ist es aber nicht mehr möglich, 3-D-Funktionen zu nutzen, wenn ein virtueller Desktop den größten Teil des Grafikspeichers belegt. Wenn die Grafikkarte beispielsweise über 16 MB RAM verfügt, kann der virtuelle Bildschirm bei einer Farbtiefe von 8 Bit bis zu 4096 x 4096 Pixel groß sein. Insbesondere bei beschleunigten Grafikkarten ist es nicht empfehlenswert, den gesamten Arbeitsspeicher für den virtuellen Bildschirm zu verwenden, weil der Kartenspeicher auch für diverse Schrift- und Grafik-Caches genutzt wird.

❼ In der Zeile Identifier (hier Screen[0]) wird für diesen Abschnitt ein Name vergeben, der als eindeutige Referenz im darauf folgenden Abschnitt ServerLayout verwendet werden kann. Die Zeilen Device und Monitor geben die Grafikkarte und den Monitor an, die zu dieser Definition gehören. Hierbei handelt es sich nur um Verbindungen zu den Abschnitten Device und Monitor mit ihren entsprechenden Namen bzw. Kennungen (*identifiers*). Diese Abschnitte werden weiter unten detailliert beschrieben.

17.1.2 Abschnitt „Device"

Im Abschnitt „Device" wird eine bestimmte Grafikkarte beschrieben. xorg.conf kann beliebig viele Grafikkarteneinträge enthalten. Jedoch muss der Name der Grafikkarten eindeutig sein. Hierfür wird das Schlüsselwort Identifier verwendet. Wenn mehrere Grafikkarten installiert sind, werden die Abschnitte einfach der Reihe nach nummeriert. Die erste wird als Device[0], die zweite als Device[1] usw. einge-

tragen. Die folgende Datei zeigt einen Auszug aus dem Abschnitt `Device` eines Computers mit einer Matrox Millennium PCI-Grafikkarte (wie von SaX2 konfiguriert):

```
Section "Device"
  BoardName      "MGA2064W"
  BusID          "0:19:0"❶
  Driver         "mga"❷
  Identifier     "Device[0]"
  VendorName     "Matrox"
  Option         "sw_cursor"
EndSection
```

❶ Der Wert unter `BusID` steht für den PCI- oder AGP-Steckplatz, in dem die Grafikkarte installiert ist. Er entspricht der ID, die bei Eingabe des Befehls `lspci` angezeigt wird. Der X-Server benötigt Informationen im Dezimalformat, `lspci` zeigt die Informationen jedoch im Hexadezimalformat an. Der Wert von `BusID` wird von SaX2 automatisch erkannt.

❷ Der Wert von `Driver` wird automatisch von SaX2 eingestellt und gibt den Treiber an, der für Ihre Grafikkarte verwendet wird. Wenn es sich um eine Matrox Millennium-Grafikkarte handelt, heißt das Treibermodul `mga`. Anschließend durchsucht der X-Server den `ModulePath`, der im Abschnitt `Files` des Unterverzeichnisses `drivers` angegeben ist. In einer Standardinstallation ist dies das Verzeichnis `/usr/lib/xorg/modules/drivers` oder das Verzeichnis `/usr/lib64/xorg/modules/drivers` für 64-Bit-Betriebssysteme. `_drv.o` wird an den Namen angehängt, sodass beispielsweise im Falle des `mga`-Treibers die Treiberdatei `mga_drv.o` geladen wird.

Das Verhalten des X-Servers bzw. des Treibers kann außerdem durch weitere Optionen beeinflusst werden. Ein Beispiel hierfür ist die Option `sw_cursor`, die im Abschnitt „Device“ festgelegt wird. Diese deaktiviert den Hardware-Mauszeiger und stellt den Mauszeiger mithilfe von Software dar. Je nach Treibermodul können verschiedene Optionen verfügbar sein. Diese finden Sie in den Beschreibungsdateien der Treibermodule im Verzeichnis `/usr/share/doc/packages/`*`Paketname`*. Allgemeingültige Optionen finden Sie außerdem auf den entsprechenden man-Seiten (`man xorg.conf`, `man 4` *`<Treibermodul>`* und `man 4` *`chips`*).

Wenn die Grafikkarte über mehrere Videoanschlüsse verfügt, können die verschiedenen an der Karte angeschlossenen Geräte in SaX2 als eine Ansicht konfiguriert werden.

17.1.3 Abschnitte „Monitor“ und „Modes“

So wie die Abschnitte vom Typ `Device` jeweils für eine Grafikkarte verwendet werden, beschreiben die Abschnitte `Monitor` und `Modes` jeweils einen Monitor. Die Konfigurationsdatei `/etc/X11/xorg.conf` kann beliebig viele Abschnitte vom Typ `Monitor` enthalten. Jeder `Monitor`-Abschnitt verweist, sofern verfügbar, auf einen `Modes`-Abschnitt mit der Zeile `UseModes`. Wenn für den Abschnitt `Monitor` kein `Modes`-Abschnitt zur Verfügung steht, berechnet der X-Server aus den allgemeinen Synchronisierungswerten passende Werte. Der Abschnitt „ServerLayout“ gibt an, welcher `Monitor`-Abschnitt zu verwenden ist.

Monitordefinitionen sollten nur von erfahrenen Benutzern festgelegt werden. Die Modelines stellen einen bedeutenden Teil der `Monitor`-Abschnitte dar. Modelines legen die horizontalen und vertikalen Frequenzen für die jeweilige Auflösung fest. Die Monitoreigenschaften, insbesondere die zulässigen Frequenzen, werden im Abschnitt `Monitor` gespeichert. Standard-VESA-Modi können auch mit dem Dienstprogramm `cvt` generiert werden. Weitere Informationen über cvt erhalten Sie auf der man-Seite `man cvt`.

WARNUNG

Die Modelines sollten Sie nur ändern, wenn Sie sich sehr gut mit den Bildschirmfunktionen und der Grafikkarte auskennen, da der Bildschirm durch eine falsche Änderung dieser Zeilen ernsthaft Schaden nehmen kann.

Falls Sie Ihre eigenen Monitorbeschreibungen entwickeln möchten, sollten Sie sich eingehend mit der Dokumentation unter `/usr/share/X11/doc` vertraut machen. Installieren Sie das Paket `xorg-x11-doc`, um PDFs und HTML-Seiten zu finden.

Heutzutage ist es nur sehr selten erforderlich, Modelines manuell festzulegen. Wenn Sie mit einem modernen Multisync-Monitor arbeiten, können die zulässigen Frequenzen und die optimalen Auflösungen in aller Regel vom X-Server direkt per DDC vom Monitor abgerufen werden, wie im SaX2-Konfigurationsabschnitt beschrieben. Ist dies aus irgendeinem Grund nicht möglich, können Sie auf einen der VESA-Modi des X-Servers zurückgreifen. Dies funktioniert in Verbindung mit den meisten Kombinationen aus Grafikkarte und Monitor.

17.2 Installation und Konfiguration von Schriften

Die Installation zusätzlicher Schriften unter SUSE Linux Enterprise Desktop ist sehr einfach. Kopieren Sie einfach die Schriften in ein beliebiges Verzeichnis im X11-Pfad für Schriften (siehe Abschnitt 17.2.1, „X11 Core-Schriften“ (S. 251)). Damit die Schriften verwendet werden können, sollte das Installationsverzeichnis ein Unterverzeichnis der Verzeichnisse sein, die in `/etc/fonts/fonts.conf` konfiguriert sind (siehe Abschnitt 17.2.2, „Xft“ (S. 252)), oder es sollte über `/etc/fonts/suse-font-dirs.conf` in diese Datei eingefügt worden sein.

Nachfolgend ein Ausschnitt aus der Datei `/etc/fonts/fonts.conf`. Diese Datei ist die Standard-Konfigurationsdatei, die für die meisten Konfigurationen geeignet ist. Sie definiert auch das eingeschlossene Verzeichnis `/etc/fonts/conf.d`. Alle Dateien und symbolischen Links in diesem Verzeichnis, die mit einer zweistelligen Zahl beginnen, werden von fontconfig geladen. Ausführliche Erläuterungen zu dieser Funktion finden Sie in der Datei `/etc/fonts/conf.d/README`.

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/.fonts</dir>
```

`/etc/fonts/suse-font-dirs.conf` wird automatisch generiert, um Schriften abzurufen, die mit Anwendungen (meist von anderen Herstellern) wie LibreOffice.org, Java oder Adobe Reader geliefert werden. Ein typischer Eintrag würde wie folgt aussehen:

```
<dir>/usr/lib/Adobe/Reader9/Resource/Font</dir>
<dir>/usr/lib/Adobe/Reader9/Resource/Font/PFM</dir>
```

Kopieren Sie zur systemweiten Installation zusätzlicher Schriften die Schriftdateien manuell (als `root`) in ein geeignetes Verzeichnis, beispielsweise `/usr/share/fonts/truetype`. Alternativ kann diese Aktion auch mithilfe des KDE-Schrift-Installationsprogramms im KDE-Kontrollzentrum durchgeführt werden. Das Ergebnis ist dasselbe.

Anstatt die eigentlichen Schriften zu kopieren, können Sie auch symbolische Links erstellen. Beispielsweise kann dies sinnvoll sein, wenn Sie lizenzierte Schriften auf einer gemounteten Windows-Partition haben und diese nutzen möchten. Führen Sie anschließend `SuSEconfig --module fonts` aus.

`SuSEconfig --module fonts` startet das für die Schriftenkonfiguration zuständige Skript `/usr/sbin/fonts-config`. Weitere Informationen zu diesem Skript finden Sie auf der man-Seite `man fonts-config`.

Die Vorgehensweise ist für Bitmap-, TrueType- und OpenType-Schriften sowie Type1-Schriften (PostScript) dieselbe. Alle diese Schriften können in einem beliebigen Verzeichnis installiert werden.

X.Org enthält zwei komplett unterschiedliche Schriftsysteme: das alte *X11-Core-Schriftsystem* und das neu entwickelte System *Xft und fontconfig*. In den folgenden Abschnitten wird kurz auf diese beiden Systeme eingegangen.

17.2.1 X11 Core-Schriften

Heute unterstützt das X11 Core-Schriftsystem nicht nur Bitmap-Schriften, sondern auch skalierbare Schriften wie Type1-, TrueType- und OpenType-Schriften. Skalierbare Schriften werden nur ohne Antialiasing und Subpixel-Rendering unterstützt und das Laden von großen skalierbaren Schriften mit Zeichen für zahlreiche Sprachen kann sehr lange dauern. Unicode-Schriften werden ebenfalls unterstützt, aber ihre Verwendung kann mit erheblichem Zeitaufwand verbunden sein und erfordert mehr Speicher.

Das X11 Core-Schriftsystem weist mehrere grundsätzliche Schwächen auf. Es ist überholt und kann nicht mehr sinnvoll erweitert werden. Zwar muss es noch aus Gründen der Abwärtskompatibilität beibehalten werden, doch das modernere System „Xft/fontconfig“ sollte immer verwendet werden, wenn es möglich ist.

Der X-Server muss die verfügbaren Schriften und deren Speicherorte im System kennen. Dies wird durch Verwendung der Variablen `FontPath` erreicht, in der die Pfade zu allen gültigen Schriftverzeichnissen des Systems vermerkt sind. In jedem dieser Verzeichnisse sind die dort verfügbaren Schriften in einer Datei mit dem Namen `fonts.dir` aufgeführt. Der `FontPath` wird vom X Server beim Systemstart erzeugt. Der Server sucht an jedem Speicherort, auf den die `FontPath`-Einträge der Konfigurationsdatei `/etc/X11/xorg.conf` verweisen, nach einer gültigen `fonts.dir`-Datei.

Diese Einträge befinden sich im Abschnitt `Files`. Der `FontPath` lässt sich mit dem Befehl `xset q` anzeigen. Dieser Pfad kann auch zur Laufzeit mit dem Befehl `xset` geändert werden. Zusätzliche Pfade werden mit `xset+fp <Pfad>` hinzugefügt. Unerwünschte Pfade können mit `xset-fp <Pfad>` gelöscht werden.

Wenn der X-Server bereits aktiv ist, können Sie neu installierte Schriften in eingehängten Verzeichnissen mit dem Befehl `xsetfp rehash` verfügbar machen. Dieser Befehl wird von `SuSEconfig--module fonts` ausgeführt. Da zur Ausführung des Befehls `xset` der Zugriff auf den laufenden X-Server erforderlich ist, ist dies nur möglich, wenn `SuSEconfig--module fonts` von einer Shell aus gestartet wird, die Zugriff auf den laufenden X-Server hat. Am einfachsten erreichen Sie dies, indem Sie `su` und das `root`-Passwort eingeben und dadurch `root`-Berechtigungen erlangen. `su` überträgt die Zugriffsberechtigungen des Benutzers, der den X Server gestartet hat, auf die `root`-Shell. Wenn Sie überprüfen möchten, ob die Schriften ordnungsgemäß installiert wurden und über das X11 Core-Schriftsystem verfügbar sind, geben Sie den Befehl `xlsfonts` ein, um alle verfügbaren Schriften aufzulisten.

Standardmäßig arbeitet SUSE Linux Enterprise Desktop mit UTF-8-Gebietsschemata. Daher sollten nach Möglichkeit Unicode-Schriften verwendet werden (Schriftnamen, die in der von `xlsfonts` ausgegebenen Liste auf `iso10646-1` enden). Alle verfügbaren Unicode-Schriften lassen sich über den Befehl `xlsfonts | grep iso10646-1` auflisten. Praktisch alle Unicode-Schriften, die unter SUSE Linux Enterprise Desktop zur Verfügung stehen, umfassen zumindest die für europäische Sprachen erforderlichen Schriftzeichen (früher als `iso-8859-*` kodiert).

17.2.2 Xft

Die Programmierer von Xft haben von Anfang an sichergestellt, dass auch skalierbare Schriften, die Antialiasing nutzen, problemlos unterstützt werden. Bei Verwendung von Xft werden die Schriften von der Anwendung, die die Schriften nutzt, und nicht vom X-Server gerendert, wie es beim X11 Core-Schriftsystem der Fall ist. Auf diese Weise hat die jeweilige Anwendung Zugriff auf die eigentlichen Schriftdateien und kann genau steuern, wie die Zeichen gerendert werden. Dies bildet eine optimale Basis für die ordnungsgemäße Textdarstellung für zahlreiche Sprachen. Direkter Zugriff auf die Schriftdateien ist sehr nützlich, wenn Schriften für die Druckausgabe eingebettet werden sollen. So lässt sich sicherstellen, dass der Ausdruck genau der Bildschirmdarstellung entspricht.

Unter SUSE Linux Enterprise Desktop nutzen die beiden Desktopumgebungen (KDE und GNOME) sowie Mozilla und zahlreiche andere Anwendungen bereits standardmäßig Xft. Xft wird inwischen von mehr Anwendungen genutzt als das alte X11 Core-Schriftsystem.

Xft greift für die Suche nach Schriften und für deren Darstellung auf die fontconfig-Bibliothek zurück. Die Eigenschaften von fontconfig werden durch die globale Konfigurationsdatei `/etc/fonts/fonts.conf` gesteuert. Spezielle Konfigurationen sollten zu `/etc/fonts/local.conf` und der benutzerspezifischen Konfigurationsdatei `~/.fonts.conf` hinzugefügt werden. Jede dieser fontconfig-Konfigurationsdateien muss folgendermaßen beginnen:

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

Enden müssen die Dateien wie folgt:

```
</fontconfig>
```

Wenn Sie möchten, dass weitere Verzeichnisse nach Schriften durchsucht werden sollen, fügen Sie Zeilen in der folgenden Weise hinzu:

```
<dir>/usr/local/share/fonts/</dir>
```

Dies ist jedoch in der Regel nicht erforderlich. Standardmäßig ist das benutzerspezifische Verzeichnis `~/.fonts` bereits in die Datei `/etc/fonts/fonts.conf` eingetragen. Entsprechend müssen Sie die zusätzlichen Schriften einfach nur nach `~/.fonts` kopieren, um sie zu installieren.

Außerdem können Sie Regeln angeben, die die Darstellung der Schriften beeinflussen. Geben Sie beispielsweise Folgendes ein:

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

Hierdurch wird das Antialiasing für alle Schriften aufgehoben. Wenn Sie hingegen

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
```

```
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

eingeben, wird das Antialiasing nur für bestimmte Schriften aufgehoben.

Standardmäßig verwenden die meisten Anwendungen die Schriftbezeichnungen `sans-serif` (bzw. `sans`), `serif` oder `monospace`. Hierbei handelt es sich nicht um eigentliche Schriften, sondern nur um Aliasnamen, die je nach Spracheinstellung in eine passende Schrift umgesetzt werden.

Benutzer können problemlos Regeln zur Datei `~/.fonts.conf` hinzufügen, damit diese Aliasnamen in ihre bevorzugten Schriften umgesetzt werden:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Da fast alle Anwendungen standardmäßig mit diesen Aliasnamen arbeiten, betrifft diese Änderung praktisch das gesamte System. Daher können Sie nahezu überall sehr einfach Ihre Lieblingsschriften verwenden, ohne die Schrifteinstellungen in den einzelnen Anwendungen ändern zu müssen.

Mit dem Befehl `fc-list` finden Sie heraus, welche Schriften installiert sind und verwendet werden können. Der Befehl `fc-list` gibt eine Liste aller Schriften zurück. Wenn Sie wissen möchten, welche der skalierbaren Schriften (`:scalable=true`) alle erforderlichen Zeichen für Hebräisch (`:lang=he`) enthalten und Sie deren Namen (`family`), Schnitt (`style`) und Stärke (`weight`) sowie die Namen der entsprechenden Schriftdateien anzeigen möchten, geben Sie folgendes Kommando ein:

```
fc-list ":lang=he:scalable=true" family style weight
```

Auf diesen Befehl kann beispielsweise Folgendes zurückgegeben werden:

```
Lucida Sans:style=Demibold:weight=200
DejaVu Sans:style=Bold Oblique:weight=200
Lucida Sans Typewriter:style=Bold:weight=200
DejaVu Sans:style=Oblique:weight=80
Lucida Sans Typewriter:style=Regular:weight=80
DejaVu Sans:style=Book:weight=80
DejaVu Sans:style=Bold:weight=200
Lucida Sans:style=Regular:weight=80
```

In der folgenden Tabelle finden Sie wichtige Parameter, die mit dem Befehl `fc-list` abgefragt werden können:

Tabelle 17.2 *Parameter zur Verwendung mit fc-list*

Parameter	Bedeutung und zulässige Werte
`family`	Der Name der Schriftamilie, z. B. `FreeSans`.
`foundry`	Der Hersteller der Schrift, z. B. `urw`.
`style`	Der Schriftschnitt, z. B. `Medium`, `Regular`, `Bold`, `Italic` oder `Heavy`.
`lang`	Die Sprache, die von dieser Schrift unterstützt wird, z. B. `de` für Deutsch, `ja` für Japanisch, `zh-TW` für traditionelles Chinesisch oder `zh-CN` für vereinfachtes Chinesisch.
`weight`	Die Schriftstärke, z. B. `80` für normale Schrift oder `200` für Fettschrift.
`slant`	Die Schriftneigung, in der Regel `0` für gerade Schrift und `100` für Kursivschrift.

Parameter	Bedeutung und zulässige Werte
geschrieben werden	Der Name der Schriftdatei.
outline	true für Konturschriften oder false für sonstige Schriften.
scalable	true für skalierbare Schriften oder false für sonstige Schriften.
bitmap	true für Bitmap-Schriften oder false für sonstige Schriften.
pixelsize	Schriftgröße in Pixel. In Verbindung mit dem Befehl „fc-list“ ist diese Option nur bei Bitmap-Schriften sinnvoll.

17.3 Weiterführende Informationen

Installieren Sie die Pakete xorg-x11-doc und howtoenh , um detailliertere Informationen zu X11 zu erhalten. Weitere Informationen zur X11-Entwicklung finden Sie auf der Startseite des Projekts unter http://www.x.org.

Viele der Treiber, die mit dem Paket xorg-x11-driver-video geliefert werden, sind ausführlich in einer man-Seite beschrieben. Wenn Sie beispielsweise den nv-Treiber verwenden, erhalten Sie weitere Informationen auf der man-Seite man 4 nv.

Informationen über Treiber von anderen Herstellern sollten in /usr/share/doc/packages/<paketname> zur Verfügung stehen. Beispielsweise ist die Dokumentation von x11-video-nvidiaG01 nach der Installation des Pakets in /usr/share/doc/packages/x11-video-nvidiaG01 verfügbar.

18 Zugriff auf Dateisysteme mit FUSE

FUSE ist das Akronym für *File System in Userspace* (Dateisystem im Benutzerraum). Das bedeutet, Sie können ein Dateisystem als nicht privilegierter Benutzer konfigurieren und einhängen. Normalerweise müssen Sie für diese Aufgabe als `root` angemeldet sein. FUSE alleine ist ein Kernel-Modul. In Kombination mit Plug-Ins kann FUSE auf nahezu alle Dateisysteme wie SSH-Fernverbindungen, ISO-Images und mehr erweitert werden.

18.1 Konfigurieren von FUSE

Bevor Sie FUSE installieren können, müssen Sie das Paket `fuse` installieren. Abhängig vom gewünschten Dateisystem benötigen Sie zusätzliche Plugins, die in verschiedenen Paketen verfügbar sind.

Im Allgemeinen müssen Sie FUSE nicht konfigurieren, Sie können es einfach verwenden. Jedoch empfiehlt es sich, ein Verzeichnis anzulegen, in dem Sie alle Ihre Einhängepunkte speichern. Sie können beispielsweise das Verzeichnis `~/mounts` anlegen und dort Ihre Unterverzeichnisse für die verschiedenen Dateisysteme einfügen.

18.2 Erhältliche FUSE-Plug-Ins

FUSE ist abhängig von Plugins. Die folgende Tabelle führt gängige Plug-Ins auf.

Tabelle 18.1 Erhältliche FUSE-Plug-Ins

`fuseiso`	Hängt CD-ROM-Images mit enthaltenen ISO9660-Dateisystemen ein.
`ntfs-3g`	Hängt NTFS-Volumes (mit Lese- und Schreibunterstützung) ein.
`sshfs`	Dateisystem-Client auf der Basis des SSH-Dateiübertragungsprotokolls
`wdfs`	Hängt WebDAV-Dateisysteme ein.

18.3 Weiterführende Informationen

Weitere Informationen finden Sie auf der Homepage `http://fuse.sourceforge.net` von FUSE.

Teil III. Mobile Computer



Mobile Computernutzung mit Linux 19

Die mobile Computernutzung wird meist mit Notebooks, PDAs, Mobiltelefonen (und dem Datenaustausch zwischen diesen Geräten) in Verbindung gebracht. An Notebooks oder Desktop-Systeme können aber auch mobile Hardware-Komponenten, wie externe Festplatten, Flash-Laufwerke und Digitalkameras, angeschlossen sein. Ebenso zählen zahlreiche Software-Komponenten zu den Bestandteilen mobiler Computerszenarien und einige Anwendungen sind sogar speziell für die mobile Verwendung vorgesehen.

19.1 Notebooks

Die Hardware von Notebooks unterscheidet sich von der eines normalen Desktopsystems. Dies liegt daran, dass Kriterien wie Austauschbarkeit, Platzanforderungen und Energieverbrauch berücksichtigt werden müssen. Die Hersteller von mobiler Hardware haben Standardschnittstellen wie PCMCIA (Personal Computer Memory Card International Association), Mini PCI und Mini PCIe entwickelt, die zur Erweiterung der Hardware von Laptops verwendet werden können. Dieser Standard bezieht sich auf Speicherkarten, Netzwerkschnittstellenkarten, ISDN (und Modemkarten) sowie externe Festplatten.

TIPP: SUSE Linux Enterprise Desktop und Tablet-PCs

SUSE Linux Enterprise Desktop unterstützt auch Tablet-PCs. Tablet PCs sind mit einem Touchpad/Grafiktablett ausgestattet. Sie können also anstatt mit Maus und Tastatur die Daten direkt am Bildschirm mit einem Grafiktablettstift oder sogar mit den Fingerspitzen bearbeiten. Installation und Konfiguration erfolgen im Großen und Ganzen wie bei jedem anderen System. Eine detaillierte Einfüh-

rung in die Installation und Konfiguration von Tablet PCs finden Sie unter Kapitel 22, *Verwenden von Tablet PCs* (S. 303).

19.1.1 Energieeinsparung

Durch die Integration von energieoptimierten Systemkomponenten bei der Herstellung von Notebooks erhöht sich die Eignung der Geräte für die Verwendung ohne Zugang zum Stromnetz. Ihr Beitrag zur Energieeinsparung ist mindestens so wichtig wie der des Betriebssystems. SUSE® Linux Enterprise Desktop unterstützt verschiedene Methoden, die den Energieverbrauch eines Notebooks beeinflussen und sich auf die Betriebsdauer bei Akkubetrieb auswirken. In der folgenden Liste werden die Möglichkeiten zur Energieeinsparung in absteigender Reihenfolge ihrer Wirksamkeit angegeben:

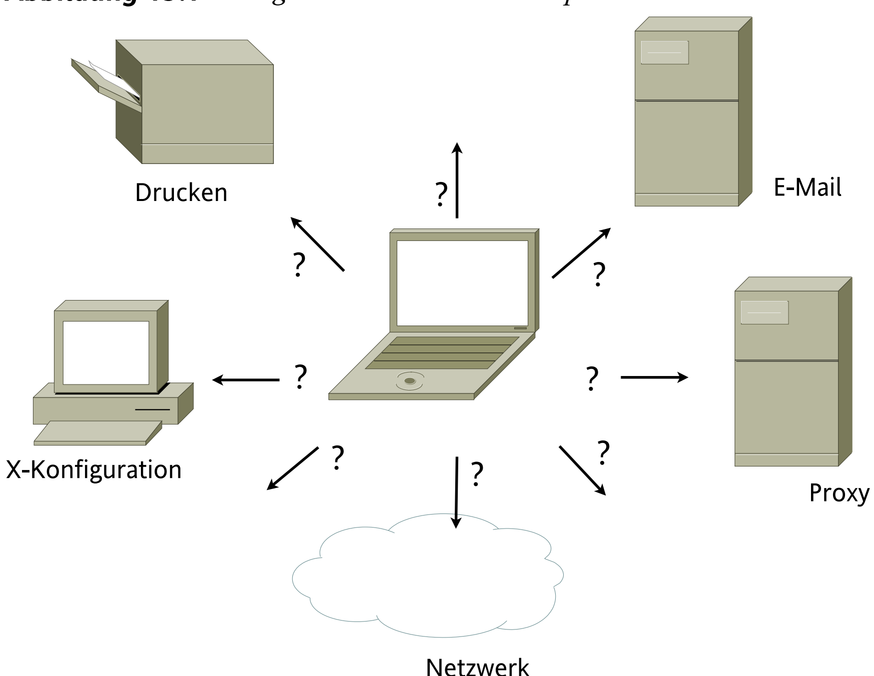
- Drosselung der CPU-Geschwindigkeit.
- Ausschalten der Anzeigebeleuchtung während Pausen.
- Manuelle Anpassung der Anzeigebeleuchtung.
- Ausstecken nicht verwendeter, Hotplug-fähiger Zubehörteile (USB-CD-ROM, externe Maus, nicht verwendete PCMCIA-Karten, WLAN usw.).
- Ausschalten der Festplatte im Ruhezustand.

Ausführliche Hintergrundinformationen zur Energieverwaltung in SUSE Linux Enterprise Desktop finden Sie in Kapitel 21, *Energieverwaltung* (S. 293). Weitere Informationen zur desktopspezifischen Energieverwaltung finden Sie unter Abschnitt „Steuerung der Desktop-Energieverwaltung“ (Kapitel 2, *Arbeiten mit dem Desktop*, ↑*GNOME-Benutzerhandbuch*) zur Verwendung der GNOME-Energieverwaltung. Weitere Informationen zum Miniprogramm für die KDE-Energieverwaltung finden Sie unter Chapter 9, *Controlling Your Desktop's Power Management* (↑*KDE User Guide*).

19.1.2 Integration in unterschiedlichen Betriebsumgebungen

Ihr System muss sich an unterschiedliche Betriebsumgebungen anpassen können, wenn es für mobile Computernutzung verwendet werden soll. Viele Dienste hängen von der Umgebung ab und die zugrunde liegenden Clients müssen neu konfiguriert werden. SUSE Linux Enterprise Desktop übernimmt diese Aufgabe für Sie.

Abbildung 19.1 *Integrieren eines mobilen Computers in eine bestehende Umgebung*



Bei einem Notebook beispielsweise, das zwischen einem kleinen Heimnetzwerk zu Hause und einem Firmennetzwerk hin und her pendelt, sind folgende Dienste betroffen:

Netzwerk
: Dazu gehören IP-Adresszuweisung, Namensauflösung, Internet-Konnektivität und Konnektivität mit anderen Netzwerken.

Druckvorgang
: Die aktuelle Datenbank der verfügbaren Drucker und ein verfügbarer Druckserver (abhängig vom Netzwerk) müssen vorhanden sein.

E-Mail und Proxys
: Wie beim Drucken muss die Liste der entsprechenden Server immer aktuell sein.

X (Grafische Umgebung)
: Wenn Ihr Notebook zeitweise an einen Projektor oder einen externen Monitor angeschlossen ist, müssen verschiedene Anzeigekonfigurationen verfügbar sein.

SUSE Linux Enterprise Desktop bietet mehrere Möglichkeiten, Laptops in vorhandene Betriebsumgebungen zu integrieren:

NetworkManager
: Der NetworkManager wurde speziell für die mobile Verbindung von Notebooks mit Netzwerken entwickelt. NetworkManager bietet die Möglichkeit, einfach und automatisch zwischen Netzwerkumgebungen oder unterschiedlichen Netzwerktypen, wie mobiles Breitband (GPRS, EDGE oder 3G), WLAN und Ethernet zu wechseln. NetworkManager unterstützt die WEP- und WPA-PSK-Verschlüsselung in drahtlosen LANs. Außerdem werden Einwahlverbindungen (mit smpppd) unterstützt. Beide Desktop-Umgebungen von SUSE Linux (GNOME und KDE) bieten ein Front-End zu NetworkManager. Weitere Informationen zu den Desktop-Applets finden Sie unter Abschnitt 26.4, „Verwenden von KNetworkManager“ (S. 404) und Abschnitt 26.5, „Verwenden des GNOME NetworkManager-Miniprogramme“ (S. 410).

Tabelle 19.1 Anwendungsbeispiele für den NetworkManager

Computer	Verwendung des NetworkManagers
Der Computer ist ein Notebook.	Ja
Der Computer wird mit verschiedenen Netzwerken verbunden.	Ja
Der Computer stellt Netzwerkdienste bereit (z. B. DNS oder DHCP).	Nein
Der Computer hat eine statische IP-Adresse.	Nein

Verwenden Sie die Werkzeuge von YaST zur Konfiguration der Netzwerkverbindungen, wenn die Netzwerkkonfiguration nicht automatisch vom NetworkManager übernommen werden soll.

TIPP: DNS-Konfiguration und verschiedene Arten von Netzwerkverbindungen

Wenn Sie oft mit Ihrem Laptop reisen und zwischen verschiedenen Arten von Netzwerkverbindungen wechseln, funktioniert NetworkManager gut, wenn alle DNS-Adressen korrekt mit DHCP zugewiesen wurden. Wenn einige Ihrer Verbindungen statische DNS-Adressen verwenden, fügen Sie NetworkManager zur Option `NETCONFIG_DNS_STATIC_SERVERS` in `/etc/sysconfig/network/config` hinzu.

SLP

Das Service Location Protocol (SLP) vereinfacht die Verbindung eines Notebooks mit einem bestehenden Netzwerk. Ohne SLP benötigt der Administrator eines Notebooks normalerweise detaillierte Kenntnisse über die im Netzwerk verfügbaren Dienste. SLP sendet die Verfügbarkeit eines bestimmten Diensttyps an alle Clients in einem lokalen Netzwerk. Anwendungen, die SLP unterstützen, können die von SLP weitergeleiteten Informationen verarbeiten und automatisch konfiguriert werden. SLP kann auch zur Installation eines Systems verwendet werden und minimiert dabei den Aufwand bei der Suche nach einer geeigneten Installations-

quelle. Weitere Informationen zu SLP finden Sie unter Kapitel 24, *SLP-Dienste im Netzwerk* (S. 387).

19.1.3 Software-Optionen

Bei der mobilen Nutzung gibt es verschiedene spezielle Aufgabenbereiche, die von dedizierter Software abgedeckt werden: Systemüberwachung (insbesondere der Ladezustand des Akkus), Datensynchronisierung sowie drahtlose Kommunikation mit angeschlossenen Geräten und dem Internet. In den folgenden Abschnitten werden die wichtigsten Anwendungen behandelt, die SUSE Linux Enterprise Desktop für jede Aufgabe bietet.

19.1.3.1 Systemüberwachung

SUSE Linux Enterprise Desktop umfasst zwei Werkzeuge zur KDE-Systemüberwachung:

Energieverwaltung
: *Power-Management* ist eine Anwendung für die Einstellung der mit der Energieeinsparung zusammenhängenden Verhaltensweisen des KDE-Desktops. Normalerweise erfolgt der Zugriff über das Symbol *Akku-Überwachung* im Systemabschnitt. Dessen Aussehen hängt vom jeweiligen Typ der Stromversorgung ab. Sie können den Konfigurationsdialog auch über den *Kickoff Application Launcher* öffnen: *Anwendungen* > *Desktop konfigurieren* > *Erweitert* > *Energiekontrolle*.

  Klicken Sie auf das Kontrollleistensymbol *Akku-Überwachung*, um auf die Optionen zur Konfiguration des Verhaltens von zuzugreifen. Sie können entsprechend Ihren Bedürfnissen eines der fünf angezeigten Energieprofile wählen. Beispiel: Das Schema *Präsentation* deaktiviert den Bildschirmschoner und das Power-Management im Allgemeinen, damit Ihre Präsentation nicht durch Systemereignisse unterbrochen wird. Klicken Sie auf *Mehr...*, um einen komplexeren Konfigurationsbildschirm zu öffnen. Hier können Sie einzelne Profile bearbeiten und erweiterte Energieverwaltungsoptionen und -benachrichtigungen festlegen, wie etwa das Verhalten bei geschlossenem Notebook oder bei niedrigem Akku-Ladezustand.

Systemmonitor
: *Systemmonitor* (auch *KSysguard*) fasst messbare Systemparameter in einer Überwachungsumgebung zusammen. Die Informationen werden standardmäßig auf zwei Registerkarten ausgegeben. *Process Table* (Prozesstabelle) enthält detaillierte

Informationen zu den aktuell ausgeführten Prozessen, wie CPU-Last, Speicherauslastung oder Prozess-ID und den Idealwert. Die Präsentation und Filterung der erfassten Daten kann angepasst werden – um einen neuen Typ von Prozessinformationen hinzuzufügen, klicken Sie mit der linken Maustaste auf die Kopfzeile der Tabelle und wählen Sie die Spalte aus, die Sie zur Ansicht hinzufügen oder daraus ausblenden möchten. Es ist auch möglich, verschiedene Systemparameter auf verschiedenen Datenseiten zu überwachen oder die Daten von mehreren Computern parallel über das Netzwerk zu sammeln. KSysguard kann außerdem als Dämon auf Computern ohne KDE-Umgebung ausgeführt werden. Weitere Informationen zu diesem Programm finden Sie in der zugehörigen integrierten Hilfefunktion bzw. auf den SUSE-Hilfeseiten.

Verwenden Sie in der GNOME-Umgebung die *Voreinstellungen für die Energieverwaltung* und den *Systemmonitor*.

19.1.3.2 Datensynchronisierung

Beim ständigen Wechsel zwischen der Arbeit auf einem mobilen Computer, der vom Netzwerk getrennt ist, und der Arbeit an einer vernetzten Arbeitsstation in einem Büro müssen die verarbeiteten Daten stets auf allen Instanzen synchronisiert sein. Dazu gehören E-Mail-Ordner, Verzeichnisse und einzelne Dateien, die sowohl für die Arbeit unterwegs als auch im Büro vorliegen müssen. Die Lösung sieht für beide Fälle folgendermaßen aus:

Synchronisieren von E-Mail

Verwenden eines IMAP-Kontos zum Speichern der E-Mails im Firmennetzwerk. Der Zugriff auf die E-Mails von der Arbeitsstation aus erfolgt dann über einen beliebigen, nicht verbundenen IMAP-fähigen E-Mail-Client, wie Mozilla Thunderbird Mail, Evolution oder KMail, wie unter *GNOME-Benutzerhandbuch* (↑*GNOME-Benutzerhandbuch*) und *KDE User Guide* (↑*KDE User Guide*) beschrieben. Der E-Mail-Client muss so konfiguriert sein, dass für `Gesendete Nachrichten` immer derselbe Ordner aufgerufen wird. Dadurch wird gewährleistet, dass nach Abschluss der Synchronisierung alle Nachrichten mit den zugehörigen Statusinformationen verfügbar sind. Verwenden Sie zum Senden von Nachrichten einen im Mail-Client implementierten SMTP-Server anstatt des systemweiten MTA-Postfix oder Sendmail, um zuverlässige Rückmeldungen über nicht gesendete Mail zu erhalten.

Synchronisieren von Dateien und Verzeichnissen
: Es gibt mehrere Dienstprogramme, die sich für die Synchronisierung von Daten zwischen Notebook und Arbeitsstation eignen. Am meisten verwendet wird ein Kommandozeilen-Tool namens `rsync`. Weitere Informationen hierzu finden Sie auf dessen man-Seite `man 1 rsync`)

19.1.3.3 Drahtlose Kommunikation

Neben einem Anschluss an ein Heim- oder Firmennetzwerk über ein Kabel kann ein Notebook für den Zugriff auf andere Computer, Peripheriegeräte, Mobiltelefone oder PDAs auch eine drahtlose Verbindung verwenden. Linux unterstützt drei Typen von drahtloser Kommunikation:

WLAN
: WLAN weist unter diesen drahtlosen Technologien die größte Reichweite auf und ist daher das einzige System, das für den Betrieb großer und zuweilen sogar räumlich getrennter Netzwerke geeignet ist. Einzelne Computer können untereinander eine Verbindung herstellen und so ein unabhängiges drahtloses Netzwerk bilden oder auf das Internet zugreifen. Als *Zugriffspunkte* bezeichnete Geräte können als Basisstationen für WLAN-fähige Geräte und als Zwischengeräte für den Zugriff auf das Internet fungieren. Ein mobiler Benutzer kann zwischen verschiedenen Zugriffspunkten umschalten, je nachdem, welcher Zugriffspunkt die beste Verbindung aufweist. Wie bei der Mobiltelefonie steht WLAN-Benutzern ein großes Netzwerk zur Verfügung, ohne dass sie für den Zugriff an einen bestimmten Standort gebunden sind. Informationen über WLAN finden Sie in Kapitel 20, *Wireless LAN* (S. 273).

Bluetooth
: Bluetooth weist das breiteste Anwendungsspektrum von allen drahtlosen Technologien auf. Es kann, ebenso wie IrDA, für die Kommunikation zwischen Computern (Notebooks) und PDAs oder Mobiltelefonen verwendet werden. Außerdem kann es zur Verbindung mehrerer Computer innerhalb des zulässigen Bereichs verwendet werden. Des Weiteren wird Bluetooth zum Anschluss drahtloser Systemkomponenten, beispielsweise Tastatur oder Maus, verwendet. Die Reichweite dieser Technologie reicht jedoch nicht aus, um entfernte Systeme über ein Netzwerk zu verbinden. WLAN ist die optimale Technologie für die Kommunikation durch physische Hindernisse, wie Wände.

IrDA
: IrDA ist die drahtlose Technologie mit der kürzesten Reichweite. Beide Kommunikationspartner müssen sich in Sichtweite voneinander befinden. Hindernisse, wie Wände, können nicht überwunden werden. Eine mögliche Anwendung von IrDA ist die Übertragung einer Datei von einem Notebook auf ein Mobiltelefon. Die kurze Entfernung zwischen Notebook und Mobiltelefon wird mit IrDa überbrückt. Der Langstreckentransport der Datei zum Empfänger erfolgt über das Mobilfunknetz. Ein weiterer Anwendungsbereich von IrDA ist die drahtlose Übertragung von Druckaufträgen im Büro.

19.1.4 Datensicherheit

Idealerweise schützen Sie die Daten auf Ihrem Notebook mehrfach gegen unbefugten Zugriff. Mögliche Sicherheitsmaßnahmen können in folgenden Bereichen ergriffen werden:

Schutz gegen Diebstahl
: Schützen Sie Ihr System stets nach Möglichkeit gegen Diebstahl. Im Einzelhandel ist verschiedenes Sicherheitszubehör, wie beispielsweise Ketten, verfügbar.

Komplexe Authentifizierung
: Verwenden Sie die biometrische Authentifizierung zusätzlich zur standardmäßigen Authentifizierung über Anmeldung und Passwort. SUSE Linux Enterprise Desktop unterstützt die Authentifizierung per Fingerabdruck. Weitere Informationen finden Sie unter Chapter 7, *Using the Fingerprint Reader* (↑*Security Guide*).

Sichern der Daten auf dem System
: Wichtige Daten sollten nicht nur während der Übertragung, sondern auch auf der Festplatte verschlüsselt sein. Dies gewährleistet die Sicherheit der Daten im Falle eines Diebstahls. Die Erstellung einer verschlüsselten Partition mit SUSE Linux Enterprise Desktop wird in Chapter 11, *Encrypting Partitions and Files* (↑*Security Guide*) beschrieben. Es ist außerdem möglich, verschlüsselte Home-Verzeichnisse beim Hinzufügen des Benutzers mit YaST zu erstellen.

WICHTIG: Datensicherheit und Suspend to Disk

Verschlüsselte Partitionen werden bei Suspend to Disk nicht ausgehängt. Daher sind alle Daten auf diesen Partitionen für jeden verfügbar, dem es

gelingt, die Hardware zu stehlen und einen Resume-Vorgang für die Festplatte durchführt.

Netzwerksicherheit
: Jeder Datentransfer muss sicher erfolgen, unabhängig von der Übertragungsart. Allgemeine, Linux und Netzwerke betreffende Sicherheitsrisiken, sind in Chapter 1, *Security and Confidentiality* (↑*Security Guide*) beschrieben. Sicherheitsmaßnahmen für drahtlose Netzwerke finden Sie in Kapitel 20, *Wireless LAN* (S. 273).

19.2 Mobile Hardware

SUSE Linux Enterprise Desktop unterstützt die automatische Erkennung mobiler Speichergeräte über FireWire (IEEE 1394) oder USB. Der Ausdruck *mobiles Speichergerät* bezieht sich auf jegliche Arten von FireWire- oder USB-Festplatten, USB-Flash-Laufwerken oder Digitalkameras. Alle Geräte werden automatisch erkannt und konfiguriert, sobald sie mit dem System über die entsprechende Schnittstelle verbunden sind. Die Dateimanager von GNOME und KDE bieten ein flexibles Arbeiten mit mobilen Hardware-Geräten. Verwenden Sie zum sicheren Aushängen dieser Medien folgende Dateiverwaltungsfunktion: *Sicher entfernen* (KDE) bzw. in GNOME die Funktion *Aushängen des Volume*. Die Handhabung von Wechselmedien wird unter *GNOME-Benutzerhandbuch* (↑*GNOME-Benutzerhandbuch*) und *KDE User Guide* (↑*KDE User Guide*) ausführlicher erläutert.

Externe Festplatten (USB und FireWire)
: Sobald eine externe Festplatte ordnungsgemäß vom System erkannt wird, wird das zugehörige Symbol in der Dateiverwaltung angezeigt. Durch Klicken auf das Symbol wird der Inhalt des Laufwerks angezeigt. Sie können hier Ordner und Dateien erstellen, bearbeiten und löschen. Um einer Festplatte einen anderen Namen zu geben als den vom System zugeteilten, wählen Sie das entsprechende Menüelement aus dem Menü aus, das beim Rechtsklicken auf das Symbol geöffnet wird. Die Namensänderung wird nur im Dateimanager angezeigt. Der Deskriptor, durch den das Gerät in `/media` eingehängt wurde, bleibt davon unbeeinflusst.

USB-Flash-Laufwerke
: Diese Geräte werden vom System genau wie externe Festplatten behandelt. Ebenso können Sie die Einträge im Dateimanager umbenennen.

Digitalkameras (USB und FireWire)
: Vom Gerät erkannte Digitalkameras werden ebenfalls im Dateimanager-Überblick als externe Laufwerke angezeigt. Mit KDE können Sie die Bilder unter URL `Kamera:/` lesen und darauf zugreifen. Diese Bilder können dann mithilfe von digiKam oder f-spot verarbeitet werden. Für die erweiterte Fotoverarbeitung steht The GIMP zur Verfügung. Eine kurze Einführung in digiKam, f-spot und The GIMP finden Sie unter Kapitel 18, *digiKam: Verwalten Ihrer digitalen Bildersammlung* (↑*Anwendungshandbuch*), Kapitel 19, *F-Spot: Verwalten Ihrer digitalen Bildersammlung* (↑*Anwendungshandbuch*) und Kapitel 17, *GIMP: Manipulieren von Grafiken* (↑*Anwendungshandbuch*).

19.3 Mobiltelefone und PDAs

Ein Desktopsystem oder Notebook kann über Bluetooth oder IrDA mit einem Mobiltelefon kommunizieren. Einige Modelle unterstützen beide Protokolle, andere nur eines von beiden. Die Anwendungsbereiche für die beiden Protokolle und die entsprechende erweiterte Dokumentation wurde bereits in Abschnitt 19.1.3.3, „Drahtlose Kommunikation“ (S. 268) erwähnt. Die Konfiguration dieser Protokolle auf den Mobiltelefonen selbst wird in den entsprechenden Handbüchern beschrieben.

Unterstützung für die Synchronisierung mit Handheld-Geräten von Palm, Inc., ist bereits in Evolution und Kontact integriert. Die erstmalige Verbindung mit dem Gerät erfolgt problemlos mit Unterstützung eines Assistenten. Sobald die Unterstützung für Palm Pilots konfiguriert wurde, müssen Sie bestimmen, welche Art von Daten synchronisiert werden soll (Adressen, Termine usw.). Weitere Informationen hierzu finden Sie unter *GNOME-Benutzerhandbuch* (↑*GNOME-Benutzerhandbuch*) und *KDE User Guide* (↑*KDE User Guide*).

Eine ausgereiftere Lösung zur Synchronisierung ist mit dem Programm `opensync` verfügbar (siehe das Paket libopensync und die entsprechenden Plugins für die verschiedenen Geräte).

19.4 Weiterführende Informationen

Die zentrale Informationsquelle für alle Fragen in Bezug auf mobile Geräte und Linux ist `http://tuxmobil.org/`. Verschiedene Bereiche dieser Website befassen sich

mit den Hardware- und Software-Aspekten von Notebooks, PDAs, Mobiltelefonen und anderer mobiler Hardware.

Einen ähnlichen Ansatz wie den unter `http://tuxmobil.org/`, finden Sie auch unter `http://www.linux-on-laptops.com/`. Hier finden Sie Informationen zu Notebooks und Handhelds.

SUSE unterhält eine deutschsprachige Mailingliste, die sich mit dem Thema Notebooks befasst. Weitere Informationen hierzu finden Sie unter `http://lists.opensuse.org/opensuse-mobile-de/`. In dieser Liste diskutieren Benutzer alle Aspekte der mobilen Computernutzung mit SUSE Linux Enterprise Desktop. Einige Beiträge sind auf Englisch, doch der größte Teil der archivierten Informationen liegt in deutscher Sprache vor. `http://lists.opensuse.org/opensuse-mobile/` ist für Beiträge in englischer Sprache vorgesehen.

Informationen über `OpenSync` finden Sie auf `http://opensync.org/`.

20 Wireless LAN

Wireless LANs oder Wireless Local Area Network (WLANs) wurden zu einem unverzichtbaren Aspekt der mobilen Datenverarbeitung. Heutzutage verfügen die meisten Notebooks über eingebaute WLAN-Karten. Dieses Kapitel beschreibt, wie Sie eine WLAN-Karte mit YaST einrichten, Übertragungen verschlüsseln und Tipps und Tricks nutzen können. Alternativ können Sie den WLAN-Zugriff mit NetworkManager konfigurieren und verwalten. Detaillierte Informationen finden Sie in Kapitel 26, *Verwendung von NetworkManager* (S. 399).

20.1 WLAN-Standards

WLAN-Karten kommunieren über den 802.11-Standard, der von der IEEE-Organisation festgelegt wurde. Ursprünglich sah dieser Standard eine maximale Übertragungsrate von 2 MBit/s vor. Inzwischen wurden jedoch mehrere Ergänzungen hinzugefügt, um die Datenrate zu erhöhen. Diese Ergänzungen definieren Details wie Modulation, Übertragungsleistung und Übertragungsraten (siehe Tabelle 20.1, „Überblick über verschiedene WLAN-Standards“ (S. 274)). Zusätzlich implementieren viele Firmen Hardware mit herstellerspezifischen Funktionen oder Funktionsentwürfen.

Tabelle 20.1 Überblick über verschiedene WLAN-Standards

Name	Band (GHz)	Maximale Übertragungsrate (MBit/s)	Hinweis
802.11 Vorläufer	2.4	2	Veraltet; praktisch keine Endgeräte verfügbar
802.11a	5	54	Weniger anfällig für Interferenzen
802.11b	2.4	11	Weniger üblich
802.11g	2.4	54	Weit verbreitet, abwärtskompatibel mit 11b
802.11n	2.4 und/oder 5	300	Common
802.11ad	2.4/5/60	bis zu 7000	2012 eingeführt, derzeit weniger üblich

802.11-Legacy-Karten werden in SUSE® Linux Enterprise Desktop nicht unterstützt. Die meisten Karten, die 802.11a-, 802.11b-, 802.11g- und 802.11n-Versionen verwenden, werden unterstützt. Neuere Karten entsprechen in der Regel dem Standard 802.11n, Karten, die 802.11g verwenden, sind jedoch noch immer erhältlich.

20.2 Betriebsmodi

Bei der Arbeit mit drahtlosen Netzwerken werden verschiedene Verfahren und Konfigurationen verwendet, um schnelle, qualitativ hochwertige und sichere Verbindungen herzustellen. Verschiedene Betriebstypen passen zu verschiedenen Einrichtungen. Die Auswahl der richtigen Authentifizierungsmethode kann sich schwierig gestalten. Die verfügbaren Verschlüsselungsmethoden weisen unterschiedliche Vor- und Nachteile auf.

Grundsätzlich lassen sich drahtlose Netzwerke in drei Netzwerkmodi klassifizieren:

Modus „Verwaltet“ (Infrastrukturmodus) über Zugriffspunkt
: Verwaltete Netzwerke verfügen über ein verwaltendes Element: den Zugriffspunkt In diesem Modus (auch als Infrastrukturmodus bezeichnet) laufen alle Verbindungen der WLAN-Stationen im Netzwerk über den Zugriffspunkt, der auch als Verbindung zu einem Ethernet fungieren kann. Um sicherzustellen, dass nur autorisierte Stationen eine Verbindung herstellen können, werden verschiedene Authentifizierungsverfahren (WPA usw.) verwendet.

Ad-hoc-Modus (Peer-To-Peer-Netzwerk)
: Ad-hoc-Netzwerke weisen keinen Zugriffspunkt auf. Die Stationen kommunizieren direkt miteinander, daher ist ein Ad-hoc-Netzwerk in der Regel schneller als ein verwaltetes Netzwerk. Übertragungsbereich und Anzahl der teilnehmenden Stationen sind jedoch in Ad-hoc-Netzwerken stark eingeschränkt. Sie unterstützen auch keine WPA-Authentifizierung. Wenn Sie WPA als Sicherheitsverfahren nutzen möchten, sollten Sie Ad-Hoc_Mode nicht verwenden.

Master-Modus
: Im Master-Modus wird Ihre Netzwerkkarte als Zugriffspunkt verwendet. Dies ist nur möglich, wenn Ihre WLAN-Karte diesen Modus unterstützt. Details zu Ihrer WLAN-Karte finden Sie unter `http://linux-wless.passys.nl`.

20.3 Authentifizierung

Da ein drahtloses Netzwerk wesentlich leichter abgehört und manipuliert werden kann als ein Kabelnetzwerk, beinhalten die verschiedenen Standards Authentifizierungs- und Verschlüsselungsmethoden. In der ursprünglichen Version von Standard IEEE 802.11 werden diese Methoden unter dem Begriff WEP (Wired Equivalent Privacy) beschrieben. Da sich WEP jedoch als unsicher herausgestellt hat (siehe Abschnitt 20.6.3, „Sicherheit“ (S. 288)), hat die WLAN-Branche (gemeinsam unter dem Namen *Wi-Fi Alliance*) die Erweiterung WPA definiert, bei dem die Schwächen von WEP ausgemerzt sein sollen. Der neuere Standard IEEE 802.11i umfasst WPA und einige andere Methoden zur Authentifizierung und Verschlüsselung. IEEE 802.11i wird mitunter auch als WPA2 bezeichnet, da WPA auf der Entwurfsversion von 802.11i basiert.

Um sicherzugehen, dass nur authentifizierte Stationen eine Verbindung herstellen können, werden in verwalteten Netzwerken verschiedene Authentifizierungsmechanismen verwendet.

Keine (offen)
Ein offenes System ist ein System, bei dem keinerlei Authentifizierung erforderlich ist. Jede Station kann dem Netzwerk beitreten. Dennoch kann die WEP-Verschlüsselung verwendet werden (siehe Abschnitt 20.4, „Verschlüsselung“ (S. 277)).

Gemeinsamer Schlüssel (gemäß IEEE 802.11)
In diesem Verfahren wird der WEP-Schlüssel zur Authentifizierung verwendet. Dieses Verfahren wird jedoch nicht empfohlen, da es den WEP-Schlüssel anfälliger für Angriffe macht. Angreifer müssen lediglich lang genug die Kommunikation zwischen Station und Zugriffspunkt abhören. Während des Authentifizierungsvorgangs tauschen beide Seiten dieselben Informationen aus, einmal in verschlüsselter, und einmal in unverschlüsselter Form. Dadurch kann der Schlüssel mit den geeigneten Werkzeugen rekonstruiert werden. Da bei dieser Methode der WEP-Schlüssel für Authentifizierung udn Verschlüsselung verwendet wird, wird die Sicherheit des Netzwerks nicht erhöht. Eine Station, die über den richtigen WEP-Schlüssel verfügt, kann Authentifizierung, Verschlüsselung und Entschlüsselung durchführen. Eine Station, die den Schlüssel nicht besitzt, kann keine empfangenden Pakete entschlüsseln. Sie kann also nicht kommunizieren, unabhängig davon, ob sie sich authentifizieren musste.

WPA-PSK (oder WPA-Personal, gemäß IEEE 802.1x)
WPA-PSK (PSK steht für „preshared key“) funktioniert ähnlich wie das Verfahren mit gemeinsamen Schlüssel. Alle teilnehmenden Stationen sowie der Zugriffspunkt benötigen denselben Schlüssel. Der Schlüssel ist 256 Bit lang und wird normalerweise als Passwortsatz eingegeben. Dieses System benötigt keine komplexe Schlüsselverwaltung wie WPA-EAP und ist besser für den privaten Gebrauch geeignet. Daher wird WPA-PSK zuweilen als WPA „Home“ bezeichnet.

WPA-EAP (oder WPA-Enterprise, gemäß IEEE 802.1x)
Eigentlich ist WPA-EAP (Extensible Authentication Protocol) kein Authentifizierungssystem, sondern ein Protokoll für den Transport von Authentifizierungsinformationen. WPA-EAP dient zum Schutz drahtloser Netzwerke in Unternehmen. Bei privaten Netzwerken wird es kaum verwendet. Aus diesem Grund wird WPA-EAP zuweilen als WPA „Enterprise“ bezeichnet.

WPA-EAP benötigt einen Radius-Server zur Authentifizierung von Benutzern. EAP bietet drei verschiedene Verfahren zur Verbindungsherstellung und Authentifizierung beim Server:

- Transport Layer Security (EAP-TLS): TLS-Authentifizierung beruht auf dem gegenseitigen Austausch von Zertifikaten für Server und Client. Zuerst legt der Server sein Zertifikat dem Client vor, der es auswertet. Wenn das Zertifikat als gültig betrachtet wird, legt im Gegenzug der Client sein eigenes Zertifikat dem Server vor. TLS ist zwar sicher, erfordert jedoch eine funktionierende Infrastruktur zur Zertifikatsverwaltung im Netzwerk. Diese Infrastruktur ist in privaten Netzwerken selten gegeben.

- Tunneled Transport Layer Security (EAP-TTSL)

- Protected Extensible Authentication Protocol (EAP-PEAP): Sowohl TTLS als auch PEAP stellen zweistufige Protokolle dar. In der ersten Stufe wird eine sichere Verbindung hergestellt und in der zweiten werden die Daten zur Client-Authentifizierung ausgetauscht. Sie erfordern einen wesentlich geringeren Zertifikatsverwaltungs-Overhead als TLS, wenn überhaupt.

20.4 Verschlüsselung

Es gibt verschiedene Verschlüsselungsmethoden, mit denen sichergestellt werden soll, dass keine nicht autorisierten Personen die in einem drahtlosen Netzwerk ausgetauschten Datenpakete lesen oder Zugriff auf das Netzwerk erlangen können:

WEP (in IEEE 802.11 definiert)

Dieser Standard nutzt den Verschlüsselungsalgorithmus RC4, der ursprünglich eine Schlüssellänge von 40 Bit aufwies, später waren auch 104 Bit möglich. Die Länge wird häufig auch als 64 Bit bzw. 128 Bit angegeben, je nachdem, ob die 24 Bit des Initialisierungsvektors mitgezählt werden. Dieser Standard weist jedoch eigene Schwächen auf. Angriffe gegen von diesem System erstellte Schlüssel können erfolgreich sein. Nichtsdestotrotz ist es besser, WEP zu verwenden, als das Netzwerk überhaupt nicht zu verschlüsseln.

Einige Hersteller haben „Dynamic WEP“ implementiert, das nicht dem Standard entspricht. Es funktioniert exakt wie WEP und weist dieselben Schwächen auf, außer dass der Schlüssel regelmäßig von einem Schlüsselverwaltungsdienst geändert wird.

TKIP (in WPA/IEEE 802.11i definiert)

Dieses im WPA-Standard definierte Schlüsselverwaltungsprotokoll verwendet denselben Verschlüsselungsalgorithmus wie WEP, weist jedoch nicht dessen

Schwächen auf. Da für jedes Datenpaket ein neuer Schlüssel erstellt wird, sind Angriffe gegen diese Schlüssel vergebens. TKIP wird in Verbindung mit WPA-PSK eingesetzt.

CCMP (in IEEE 802.11i definiert)
: CCMP beschreibt die Schlüsselverwaltung. Normalerweise wird sie in Verbindung mit WPA-EAP verwendet, sie kann jedoch auch mit WPA-PSK eingesetzt werden. Die Verschlüsselung erfolgt gemäß AES und ist stärker als die RC4-Verschlüsselung des WEP-Standards.

20.5 Konfiguration mit YaST

WICHTIG: Sicherheitsrisiken in drahtlosen Netzwerken.

Bei nicht verschlüsselten WLAN-Verbindungen können Dritte alle Netzwerkdaten abfangen. Schützen Sie Ihren Netzwerkverkehr unbedingt mit einer der unterstützten Methoden zur Authentifizierung und Verschlüsselung.

Verwenden Sie die bestmögliche Verschlüsselungsmethode, die Ihre Hardware zulässt. Eine bestimmte Verschlüsselungsmethode muss jedoch von allen Geräten im Netzwerk unterstützt werden. Andernfalls können die Geräte nicht miteinander kommunizieren. Wenn Ihr Router z. B. sowohl WEP als auch WPA, der Treiber für Ihre WLAN-Karte jedoch nur WEP unterstützt, stellt WEP den kleinsten gemeinsamen Nenner dar, den Sie verwenden können. Doch selbst eine schwache Verschlüsselung mit WEP ist besser als gar keine. Weitere Informationen hierzu erhalten Sie in Abschnitt 20.4, „Verschlüsselung“ (S. 277) und Abschnitt 20.6.3, „Sicherheit“ (S. 288).

Um ein WLAN mit YaST zu konfigurieren, müssen folgende Parameter definiert werden:

IP-Adresse
: Verwenden Sie entweder eine statische IP-Adresse oder nehmen Sie mit einem DHCP-Server eine dynamische Zuweisung einer IP-Adresse zur Schnittstelle vor.

Betriebsmodus
: Definiert, wie Ihr Rechner abhängig von der Netzwerktopologie in ein WLAN integriert wird. Hintergrundinformationen zu erhalten Sie in Abschnitt 20.2, „Betriebsmodi“ (S. 274).

Netzwerkname (ESSID)
: Eindeutige Zeichenkette zur Identifizierung eines Netzwerks.

Details zur Authentifizierung und Verschlüsselung
: Abhängig von der von Ihrem Netzwerk verwendeten Authentifizierungs- und Verschlüsselungsmethode muss mindestens ein Schlüssel bzw. Zertifikat eingegeben werden.

  Zur Eingabe der entsprechenden Schlüssel stehen verschiedene Eingabeoptionen zur Verfügung: *Passphrase*, *ASCII* (nur für WEP-Authentifizierungsmethoden verfügbar) und *Hexadezimal*.

20.5.1 Deaktivieren von NetworkManager

Eine WLAN-Karte wird gewöhnlich während der Installation erkannt. Handelt es sich bei Ihrem Rechner um einen mobilen Computer, wird NetworkManager im Normalfall standardmäßig aktiviert. Wenn Sie Ihre WLAN-Karte stattdessen mit YaST konfigurieren möchten, müssen Sie NetworkManager zunächst deaktivieren:

1. Starten Sie YaST als `root`.

2. Wählen Sie im YaST-Kontrollzentrum die Option *Netzwerkgeräte* > *Netzwerkeinstellungen*. Das Dialogfeld *Netzwerkeinstellungen* wird geöffnet.

   Wird Ihr Netzwerk zurzeit von NetworkManager gesteuert, wird eine Warnmeldung mit dem Hinweis angezeigt, dass die Netzwerkeinstellungen von YaST nicht bearbeitet werden können.

3. Zum Aktivieren der Bearbeitung mit YaST beenden Sie die Meldung durch Klicken auf *OK* und aktivieren Sie auf dem Karteireiter *Globale Optionen* die Option *Traditionelle Methode mit ifup*.

4. Zur weiteren Konfiguration fahren Sie mit Abschnitt Abschnitt 20.5.2, „Konfiguration für Zugriffspunkte“ (S. 280) oder Abschnitt 20.5.3, „Einrichten eines Ad-hoc-Netzwerks“ (S. 284) fort.

   Bestätigen Sie andernfalls Ihre Änderungen mit *OK*, um die Netzwerkkonfiguration zu schreiben.

20.5.2 Konfiguration für Zugriffspunkte

In diesem Abschnitt erfahren Sie, wie Sie Ihre WLAN-Karte für die Verbindung mit einem (externen) Zugriffspunkt konfigurieren bzw. wie Sie Ihre WLAN-Karte als Zugriffspunkt verwenden, sofern diese Funktion von Ihrer WLAN-Karte unterstützt wird. Informationen zur Konfiguration von Netzwerken ohne Zugriffspunkt finden Sie unter Abschnitt 20.5.3, „Einrichten eines Ad-hoc-Netzwerks“ (S. 284).

Prozedur 20.1 *Konfigurieren Ihrer WLAN-Karte zur Verwendung eines Zugriffspunkts*

1 Starten Sie YaST und öffnen Sie das Dialogfeld *Netzwerkeinstellungen*.

2 Wechseln Sie zur Registerkarte *Übersicht*, auf der alle vom System erkannten Netzwerkkarten aufgelistet sind. Wenn Sie weitere Informationen über die allgemeine Netzwerkkonfiguration benötigen, schlagen Sie unter Abschnitt 23.4, „Konfigurieren von Netzwerkverbindungen mit YaST“ (S. 337) nach.

3 Wählen Sie die drahtlose Karte aus der Liste aus und klicken Sie auf *Bearbeiten*, um das Dialogfeld „Einrichten von Netzwerkkarten“ zu öffnen.

4 Legen Sie auf dem Karteireiter *Adresse* fest, ob eine dynamische oder eine statische IP-Adresse für den Rechner verwendet werden soll. In den meisten Fällen ist die *Dynamische Adresse* mit *DHCP* geeignet.

5 Klicken Sie auf *Weiter*, um mit dem Dialogfeld *Konfiguration der drahtlosen Netzwerkkarte* fortzufahren.

6 Um Ihre WLAN-Karte zur Verbindung mit einem Zugriffspunkt zu verwenden, legen Sie den *Betriebsmodus* auf *Verwaltet* fest.

Falls Sie Ihre WLAN-Karte hingegen als Zugriffspunkt verwenden möchten, legen Sie den *Betriebsmodus* auf *Master* fest. Beachten Sie, dass dieser Modus nicht von allen WLAN-Karten unterstützt wird.

ANMERKUNG: Verwenden von WPA-PSK oder WPA-EAP

Bei Verwendung der Authentifizierungsmethode WPA-PSK oder WPA-EAP muss der Betriebsmodus auf *Verwaltet* eingestellt sein.

---

7 Zum Herstellen einer Verbindung mit einem bestimmten Netzwerk geben Sie den entsprechenden *Netzwerknamen (ESSID)* ein. Sie können stattdessen auch auf *Netzwerk durchsuchen* klicken und ein Netzwerk in der Liste der verfügbaren drahtlosen Netzwerke auswählen.

   Alle Stationen in einem drahtlosen Netzwerk benötigen dieselbe ESSID zur Kommunikation untereinander. Ist keine ESSID angegeben, stellt Ihre WLAN-Karte automatisch eine Verbindung zu dem Zugriffspunkt mit der besten Signalstärke her.

   ANMERKUNG: Notwendigkeit der ESSID für die WPA-Authentifizierung

   Bei Auswahl der *WPA*-Authentifizierung muss ein Netzwerkname (ESSID) festgelegt werden.

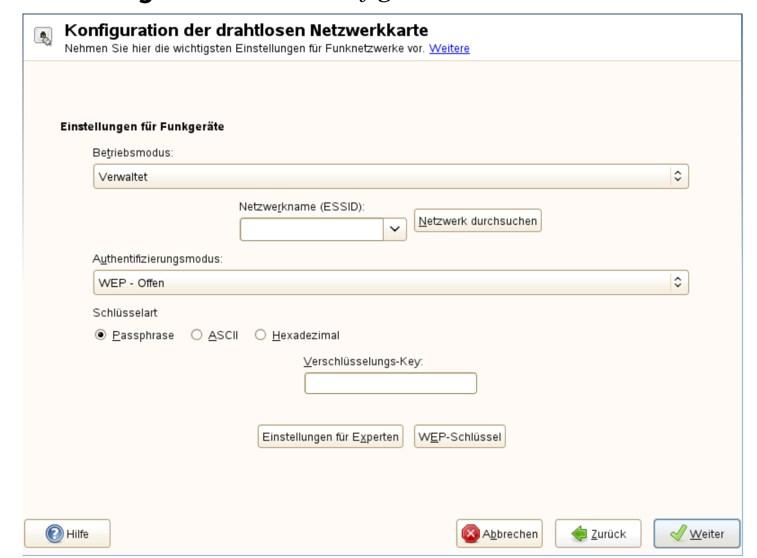
   ---

8 Wählen Sie einen *Authentifizierungsmodus* für Ihr Netzwerk aus. Welcher Modus geeignet ist, hängt vom Treiber Ihrer WLAN-Karte und von der Fähigkeit der anderen Geräte im Netzwerk ab.

9 Wenn Sie den *Authentifizierungsmodus* auf *Keine Verschlüsselung* festgelegt haben, schließen Sie die Konfiguration durch Klicken auf *Weiter* ab. Bestätigen Sie die Meldung zu diesem potenziellen Sicherheitsrisiko und verlassen Sie den Karteireiter *Übersicht* (über die neu konfigurierte WLAN-Karte) durch Klicken auf *OK*.

   Wenn Sie eine der anderen Authentifizierungsmodi ausgewählt haben, fahren Sie mit Prozedur 20.2, „Eingeben der Verschlüsselungsdetails“ (S. 282) fort.

Abbildung 20.1 *YaST: Konfigurieren der WLAN-Karte*



Prozedur 20.2 *Eingeben der Verschlüsselungsdetails*

Für die folgenden Authentifizierungsmethoden ist ein Verschlüsselungs-Key erforderlich: *WEP - Offen*, *WEP - Gemeinsamer Schlüssel* und *WPA-PSK*.

Für WEP ist im Normalfall nur ein Schlüssel erforderlich. Sie können jedoch für Ihre Station bis zu 4 verschiedene WEP-Schlüssel definieren. Einer der Schlüssel muss als Standardschlüssel festgelegt werden und wird für die Verschlüsselung verwendet. Die anderen dienen zur Entschlüsselung. Standardmäßig wird eine Schlüssellänge von 128-Bit verwendet. Sie können die Länge jedoch auch auf 64-Bit festlegen.

Zur Verbesserung der Sicherheit verwendet WPA-EAP einen RADIUS-Server zur Benutzerauthentifizierung. Zur serverseitigen Authentifizierung sind drei verschiedene Methoden verfügbar: TLS, TTLS und PEAP. Die für WPA-EAP erforderlichen Berechtigungsnachweise und Zertifikate hängen davon ab, welche Authentifizierungsmethode für den RADIUS-Server verwendet wird. Die benötigten Informationen und Berechtigungsnachweise erhalten Sie von Ihrem Systemadministrator. YaST sucht unter `/etc/cert` nach einem Zertifikat. Speichern Sie daher die erhaltenen Zertifikate an diesem Ort und schränken Sie den Zugriff zu diesen Dateien auf `0600` (Lese- und Schreibzugriff des Eigentümers) ein.

1 So geben Sie den Schlüssel für *WEP - Offen* oder *WEP - Gemeinsamer Schlüssel* ein:

1a Legen Sie die *Schlüsselart* entweder auf *Passphrase*, *ASCII* oder *Hexadezimal* fest.

1b Geben Sie den entsprechenden *Verschlüsselungs-Key* ein (im Normalfall wird nur ein Schlüssel verwendet):

Bei Auswahl von *Passphrase* geben Sie ein Wort oder eine Zeichenkette ein, mit dem bzw. der ein Schlüssel mit der angegebenen Schlüssellänge (standardmäßig 128-Bit) generiert wird.

ASCII erfordert die Eingabe von 5 Zeichen für einen 64-Bit-Schlüssel und von 13 Zeichen für einen 128-Bit-Schlüssel.

Bei *Hexadezimal* geben Sie 10 Zeichen für einen 64-Bit-Schlüssel bzw. 26 Zeichen für einen 128-Bit-Schlüssel in Hexadezimalnotation ein.

1c Zum Anpassen der Schlüssellänge an eine niedrigere Bitrate (u. U. für ältere Hardware erforderlich) klicken Sie auf *WEP-Schlüssel* und legen Sie die *Schlüssellänge* auf *64* Bit fest. Im Dialogfeld *WEP-Schlüssel* werden außerdem die WEP-Schlüssel angezeigt, die bis dahin eingegeben wurden. Sofern kein anderer Schlüssel explizit als Standard festgelegt wurde, verwendet YaST immer den ersten Schlüssel als Standardschlüssel.

1d Um weitere Schlüssel für WEP einzugeben oder einen der Schlüssel zu ändern, wählen Sie den entsprechenden Eintrag aus und klicken Sie auf *Bearbeiten*. Wählen Sie die *Schlüsselart* aus und geben Sie den Schlüssel ein.

1e Bestätigen Sie die Änderungen mit *OK*.

2 So geben Sie einen Schlüssel für *WPA-PSK* ein:

2a Wählen Sie die Eingabemethode *Passphrase* oder *Hexadezimal* aus.

2b Geben Sie den entsprechenden *Verschlüsselungs-Key* ein.

Im Modus *Passwortsatz* muss die Eingabe 8 bis 63 Zeichen betragen. Im Modus *Hexadezimal* geben Sie 64 Zeichen ein.

3 Bei Auswahl der *WPA-EAP*-Authentifizierung klicken Sie auf *Weiter*, um zum Dialogfeld *WPA-EAP* zu wechseln. Geben Sie hier die Berechtigungsnachweise und Zertifikate ein, die Sie von Ihrem Netzwerkadministrator erhalten haben.

  3a Wählen Sie den *EAP-Modus* aus, der vom RADIUS-Server zur Authentifizierung verwendet wird. Die im Folgenden einzugebenden Details hängen vom ausgewählten *EAP-Modus* ab.

  3b Geben Sie für TLS *Identität*, *Client-Zertifikat*, *Client-Schlüssel* und *Client-Schlüssel-Passwort* an. Zur Verbesserung der Sicherheit können Sie außerdem ein *Server-Zertifikat* konfigurieren, mit dem die Authentizität des Servers validiert wird.

  Für TTLS und PEAP sind *Identität* und *Passwort* erforderlich, während *Server-Zertifikat* und *Anonyme Identität* optional sind.

  3c Klicken Sie auf *Details*, um im Dialogfeld für die erweiterte Authentifizierung Daten für Ihre WPA-EAP-Einrichtung einzugeben.

  3d Wählen Sie die *Authentifizierungsmethode* für die zweite Phase der EAP-TTLS- oder EAP-PEAP-Kommunikation (innere Authentifizierung) aus. Die verfügbaren Methoden hängen von der Authentifizierungsmethode für den RADIUS-Server ab, die Sie im vorherigen Dialogfeld ausgewählt haben.

  3e Wenn die automatisch festgelegte Einstellung nicht ausreicht, wählen Sie eine bestimmte *PEAP-Version*, um die Verwendung einer spezifischen PEAP-Installation zu erzwingen.

4 Bestätigen Sie die Änderungen mit *OK*. Der Karteireiter *Übersicht* zeigt die Details Ihrer neu konfigurierten WLAN-Karte.

5 Klicken Sie auf *OK*, um die Konfiguration abzuschließen und das Dialogfeld zu schließen.

20.5.3 Einrichten eines Ad-hoc-Netzwerks

In einigen Fällen ist es sinnvoll, zwei Computer zu verbinden, die mit einer WLAN-Karte ausgestattet sind. So richten Sie ein Ad-hoc-Netzwerk mit YaST ein:

1. Starten Sie YaST und öffnen Sie das Dialogfeld *Netzwerkeinstellungen*.

2. Wechseln Sie zum Karteireiter *Übersicht*, wählen Sie Ihre drahtlose Karte in der Liste aus und klicken Sie auf *Bearbeiten*, um das Dialogfeld *Netzwerkkarte einrichten* zu öffnen.

3. Wählen Sie *Statisch zugewiesene IP-Adresse* und geben Sie die folgenden Daten ein:

   - *IP-Adresse:* `192.168.1.1`. Ändern Sie diese Adresse auf dem zweiten Computer beispielsweise in `192.168.1.2`.

   - *Subnetz-Maske*: `/24`

   - *Hostname*: Wählen Sie einen Namen nach Belieben.

4. Fahren Sie mit *Weiter* fort.

5. Legen Sie den *Betriebsmodus* auf *Ad-hoc* fest.

6. Wählen Sie einen *Netzwerknamen (ESSID)*. Dies kann ein beliebiger Name sein, jedoch muss er auf jedem Computer des Ad-hoc-Netzwerks benutzt werden.

7. Wählen Sie einen *Authentifizierungsmodus* für Ihr Netzwerk aus. Welcher Modus geeignet ist, hängt vom Treiber Ihrer WLAN-Karte und von der Fähigkeit der anderen Geräte im Netzwerk ab.

8. Wenn Sie den *Authentifizierungsmodus* auf *Keine Verschlüsselung* festgelegt haben, schließen Sie die Konfiguration durch Klicken auf *Weiter* ab. Bestätigen Sie die Meldung zu diesem potenziellen Sicherheitsrisiko und verlassen Sie den Karteireiter *Übersicht* über die neu konfigurierte WLAN-Karte durch Klicken auf *OK*.

   Wenn Sie eine der anderen Authentifizierungsmodi ausgewählt haben, fahren Sie mit Prozedur 20.2, „Eingeben der Verschlüsselungsdetails“ (S. 282) fort.

9. Wenn `smpppd` nicht installiert ist, fordert Sie YaST dazu auf.

10 Konfigurieren Sie die anderen WLAN-Karten im Netzwerk entsprechend mit dem gleichen *Netzwerknamen (ESSID)*, dem gleichen *Authentifizierungsmodus*, jedoch unterschiedlichen IP-Adressen.

20.5.4 Festlegen zusätzlicher Konfigurationsparameter

Im Normalfall müssen die vorkonfigurierten Einstellungen beim Konfigurieren Ihrer WLAN-Karte nicht geändert werden. Wenn Sie jedoch eine detaillierte Konfiguration Ihrer WLAN-Verbindung benötigen, ermöglicht YaST eine Feineinstellung folgender Optionen:

Channel
: Die Angabe eines Kanals, auf dem die WLAN-Station arbeiten sollte. Diese Angabe ist nur in den Modi *Ad-hoc* und *Master* erforderlich. Im Modus *Verwaltet* durchsucht die Karte automatisch die verfügbaren Kanäle nach Zugriffspunkten.

Bitrate
: Je nach der Leistungsfähigkeit Ihres Netzwerks können Sie eine bestimmte Bitrate für die Übertragung von einem Punkt zum anderen festlegen. Bei der Standardeinstellung, *Auto*, versucht das System, die höchstmögliche Datenübertragungsrate zu verwenden. Einige WLAN-Karten unterstützen die Festlegung von Bitraten nicht.

Zugriffspunkt
: In einer Umgebung mit mehreren Zugriffspunkten kann einer davon durch Angabe der MAC-Adresse vorausgewählt werden.

Energieverwaltung
: Wenn Sie Ihr Notebook unterwegs verwenden, sollten Sie die Akku-Betriebsdauer mithilfe von Energiespartechnologien maximieren. Weitere Informationen über die Energieverwaltung finden Sie in Kapitel 21, *Energieverwaltung* (S. 293). Die Verwendung der Energieverwaltung kann die Verbindungsqualität beeinflussen und die Netzwerklatenz erhöhen.

So greifen Sie auf erweiterte Optionen zu:

1 Starten Sie YaST und öffnen Sie das Dialogfeld *Netzwerkeinstellungen*.

2 Wechseln Sie zum Karteireiter *Übersicht*, wählen Sie Ihre drahtlose Karte in der Liste aus und klicken Sie auf *Bearbeiten*, um das Dialogfeld *Netzwerkkarte einrichten* zu öffnen.

3 Klicken Sie auf *Weiter*, um mit dem Dialogfeld *Konfiguration der drahtlosen Netzwerkkarte* fortzufahren.

4 Klicken Sie auf *Einstellungen für Experten*.

5 Im Modus *Ad-hoc* müssen Sie einen der angebotenen Kanäle (11 bis 14, abhängig von Ihrem Land) für die Kommunikation zwischen Ihrer Station und den anderen Stationen auswählen. Im Modus *Master* müssen Sie festlegen, auf welchem *Kanal* Ihre Karte die Funktionen des Zugriffspunkts anbieten soll. Die Standardeinstellung für diese Option lautet *Auto*.

6 Wählen Sie die zu verwendende *Bitrate* aus.

7 Geben Sie die MAC-Adresse des *Zugriffspunkts* ein, mit dem Sie eine Verbindung herstellen möchten.

8 Aktivieren bzw. deaktivieren Sie die Option *Power-Management verwenden*.

9 Bestätigen Sie Ihre Änderungen mit *OK* und klicken Sie auf *Weiter* und auf *OK*, um die Konfiguration abzuschließen.

20.6 Tipps und Tricks zur Einrichtung eines WLAN

Die folgenden Tools und Tipps können Sie bei der Überwachung und Verbesserung der Geschwindigkeit und Stabilität sowie von Sicherheitsaspekten unterstützen.

20.6.1 Dienstprogramme

Das Paket `wireless-tools` enthält Dienstprogramme, mit denen Sie Wireless-LAN-spezifische Parameter festlegen und Statistiken abrufen können. Weitere Informa-

tionen finden Sie unter http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html.

20.6.2 Stabilität und Geschwindigkeit

Leistungsfähigkeit und Zuverlässigkeit eines drahtlosen Netzwerks hängen in erster Linie davon ab, ob die teilnehmenden Stationen ein klares Signal von den anderen Stationen empfangen. Hindernisse, wie beispielsweise Wände, schwächen das Signal erheblich ab. Je weiter die Signalstärke sinkt, desto langsamer wird die Übertragung. Während des Betriebs können Sie die Signalstärke mit dem Dienstprogramm `iwconfig` in der Kommandozeile (Feld `Link-Qualität`) oder mit dem NetworkManager-Miniprogramm aus KDE oder GNOME überprüfen. Bei Problemen mit der Signalqualität sollten Sie versuchen, die Geräte an einer anderen Position einzurichten oder die Antennen der Zugriffspunkte neu zu positionieren. Hilfsantennen, die den Empfang erheblich verbessern sind für eine Reihe von PCMCIA-WLAN-Karten erhältlich. Die vom Hersteller angegebene Rate, beispielsweise 54 MBit/s, ist ein Nennwert, der für das theoretische Maximum steht. In der Praxis beträgt der maximale Datendurchsatz nicht mehr als die Hälfte dieses Werts.

Mit dem Kommando `iwspy` können WLAN-Statistiken angezeigt werden:

```
iwspy wlan0
wlan0      Statistics collected:
    00:AA:BB:CC:DD:EE : Quality:0  Signal level:0  Noise level:0
   Link/Cell/AP      : Quality:60/94  Signal level:-50 dBm   Noise level:-140
 dBm (updated)
   Typical/Reference : Quality:26/94  Signal level:-60 dBm   Noise level:-90
 dBm
```

20.6.3 Sicherheit

Wenn Sie ein drahtloses Netzwerk einrichten möchten, sollten Sie bedenken, dass jeder, der sich innerhalb der Übertragungsreichweite befindet, problemlos auf das Netzwerk zugreifen kann, sofern keine Sicherheitsmaßnahmen implementiert sind. Daher sollten Sie auf jeden Fall eine Verschlüsselungsmethode aktivieren. Alle WLAN-Karten und Zugriffspunkte unterstützen WEP-Verschlüsselung. Dieses Verfahren bietet zwar keine absolute Sicherheit, es stellt jedoch durchaus ein Hindernis für mögliche Angreifer dar.

Verwenden Sie für private Zwecke WPA-PSK, sofern verfügbar. Linux unterstützt zwar WPA auf den meisten Hardwarekomponenten, jedoch bieten einige Treiber keine

WPA-Unterstützung. Diese ist auf älteren Zugriffspunkten und Routern mit WLAN-Funktionen möglicherweise auch nicht verfügbar. Überprüfen Sie für derartige Geräte, ob WPA mithilfe eines Firmware-Updates installiert werden kann. Wenn WPA nicht verfügbar ist, sollten Sie lieber WEP verwenden, als völlig auf Verschlüsselung zu verzichten. Bei Unternehmen mit erhöhten Sicherheitsanforderungen sollten drahtlose Netzwerke ausschließlich mit WPA betrieben werden.

Verwenden Sie für Ihre Authentifizierungsmethode sichere Passwörter. Die Webseite `https://www.grc.com/passwords.htm` generiert zum Beispiel Zufallspasswörter mit einer Länge von 64 Zeichen.

20.7 Fehlersuche

Wenn Ihre WLAN-Karte nicht antwortet, überprüfen Sie folgende Voraussetzungen:

1. Ist Ihnen der Gerätename der WLAN-Karte bekannt? Dieser lautet in der Regel `wlan0`. Überprüfen Sie den Namen mit dem Tool `ifconfig`.

2. Haben Sie sichergestellt, dass die erforderliche Firmware vorhanden ist? Weitere Informationen finden Sie in `/usr/share/doc/packages/wireless-tools/README.firmware`.

3. Wird die ESSID Ihres Routers via Broadcast übermittelt und ist sie sichtbar (d. h. nicht versteckt)?

20.7.1 Netzwerkstatus überprüfen

Mit dem Kommando `iwconfig` können Sie nützliche Informationen zu Ihrer drahtlosen Verbindung abrufen. Die folgende Zeile gibt zum Beispiel die ESSID, den drahtlosen Modus, die Frequenz, die Verbindungsqualität, ob Ihr Signal verschlüsselt ist und vieles mehr an:

```
iwconfig wlan0
wlan0  IEEE 802.11abg  ESSID:"guest"
       Mode:Managed   Frequency:5.22GHz  Access Point: 00:11:22:33:44:55
       Bit Rate:54 Mb/s   Tx-Power=13 dBm
       Retry min limit:7   RTS thr:off   Fragment thr:off
       Encryption key:off
       Power Management:off
       Link Quality:62/92   Signal level:-48 dBm  Noise level:-127 dBm
```

```
       Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
       Tx excessive retries:10  Invalid misc:0   Missed beacon:0
```

Die gleichen Informationen können Sie auch mit dem Kommando `iwlist` abrufen. Die folgende Zeile gibt zum Beispiel die aktuelle Bitrate an:

```
iwlist wlan0 rate
wlan0    unknown bit-rate information.
         Current Bit Rate=54 Mb/s
```

Eine Übersicht über die Anzahl der verfügbaren Zugriffspunkte erhalten Sie auch mit dem Kommando `iwlist`. Dieses Kommando ruft eine Liste mit „Zellen“ ab, die wie folgt aussieht:

```
iwlist wlan0 scanning
wlan0   Scan completed:
   Cell 01 - Address: 00:11:22:33:44:55
             Channel:40
             Frequency:5.2 GHz (Channel 40)
             Quality=67/70  Signal level=-43 dBm
             Encryption key: off
             ESSID:"Guest"
             Bit Rates: 6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s;
                        24 Mb/s; 36 Mb/s; 48 Mb/s
             Mode: Master
             Extra:tsf=0000111122223333
             Extra: Last beacon: 179ms ago
             IE: Unknown: ...
```

20.7.2 Mehrere Netzwerkgeräte

Moderne Laptops verfügen normalerweise über eine Netzwerkkarte und eine WLAN-Karte. Wenn Sie beide Geräte mit DHCP (automatische Adresszuweisung) konfiguriert haben, können Probleme mit der Namenauflösung und dem Standard-Gateway auftreten. Dies können Sie daran erkennen, dass Sie dem Router ein Ping-Signal senden, jedoch nicht das Internet verwenden können. In der Support-Datenbank finden Sie unter http://old-en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients einen Artikel zu diesem Thema.

20.7.3 Probleme mit Prism2-Karten

Für Geräte mit Prism2-Chips sind mehrere Treiber verfügbar. Die verschiedenen Karten funktionieren mit den einzelnen Treibern mehr oder weniger reibungslos. Bei diesen Karten ist WPA nur mit dem hostap-Treiber möglich. Wenn eine solche Karte nicht einwandfrei oder überhaupt nicht funktioniert oder Sie WPA verwenden möchten, lesen Sie nach unter `/usr/share/doc/packages/wireless-tools/README.prism2`.

20.8 Weiterführende Informationen

Weitere Informationen finden Sie auf den folgenden Seiten:

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html
: Auf den Internetseiten von Jean Tourrilhes, dem Entwickler der *Wireless Tools* für Linux finden Sie ein breites Spektrum an nützlichen Informationen zu drahtlosen Netzwerken.

http://tuxmobil.org
: Nützliche und praktische Informationen über mobile Computer unter Linux.

http://www.linux-on-laptops.com
: Weitere Informationen zu Linux auf Notebooks.



21 Energieverwaltung

Die Energieverwaltung ist insbesondere bei Notebook-Computern von großer Wichtigkeit, sie ist jedoch auch für andere Systeme sinnvoll. ACPI (Advanced Configuration & Power Interface) ist auf allen modernen Computern (Laptops, Desktops, Server) verfügbar. Für Energieverwaltungstechnologien sind geeignete Hardware- und BIOS-Routinen erforderlich. Die meisten Notebooks und modernen Desktops und Server erfüllen diese Anforderungen. Es ist außerdem möglich, die CPU-Frequenzskalierung zu steuern, um Energie zu sparen oder den Geräuschpegel zu senken.

21.1 Energiesparfunktionen

Energiesparfunktionen sind nicht nur für die mobile Verwendung von Notebooks von Bedeutung, sondern auch für Desktop-Systeme. Die Hauptfunktionen und ihre Verwendung im ACPI sind:

Standby
: Nicht unterstützt.

Stromsparmodus (in Speicher)
: In diesem Modus wird der gesamte Systemstatus in den RAM geschrieben. Anschließend wird das gesamte System mit Ausnahme des RAM in den Ruhezustand versetzt. In diesem Zustand verbraucht der Computer sehr wenig Energie. Der Vorteil dieses Zustands besteht darin, dass innerhalb weniger Sekunden die Arbeit nahtlos wieder aufgenommen werden kann, ohne dass ein Booten des Systems oder ein Neustart der Anwendungen erforderlich ist. Diese Funktion entspricht ACPI-Zustand `S3`.

Tiefschlaf (Suspend to Disk)
: In diesem Betriebsmodus wird der gesamte Systemstatus auf die Festplatte geschrieben und das System wird von der Energieversorgung getrennt. Es muss eine Swap-Partition vorhanden sein, die mindestens die Größe des RAM hat, damit alle aktiven Daten geschrieben werden können. Die Reaktivierung von diesem Zustand dauert ungefähr 30 bis 90 Sekunden. Der Zustand vor dem Suspend-Vorgang wird wiederhergestellt. Einige Hersteller bieten Hybridvarianten dieses Modus an, beispielsweise RediSafe bei IBM Thinkpads. Der entsprechende ACPI-Zustand ist `S4`. In Linux wird „suspend to disk“ über Kernel-Routinen durchgeführt, die von ACPI unabhängig sind.

Akku-Überwachung
: ACPI überprüft den Akkuladestatus und stellt entsprechende Informationen bereit. Außerdem koordiniert es die Aktionen, die beim Erreichen eines kritischen Ladestatus durchzuführen sind.

Automatisches Ausschalten
: Nach dem Herunterfahren wird der Computer ausgeschaltet. Dies ist besonders wichtig, wenn der Computer automatisch heruntergefahren wird, kurz bevor der Akku leer ist.

Steuerung der Prozessorgeschwindigkeit
: In Verbindung mit der CPU gibt es drei Möglichkeiten, Energie zu sparen: Frequenz- und Spannungsskalierung (auch PowerNow! oder Speedstep), Drosselung und Versetzen des Prozessors in den Ruhezustand (C-Status). Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden.

21.2 Advanced Configuration & Power Interface (ACPI)

Die ACPI (erweiterte Konfigurations- und Energieschnittstelle) wurde entwickelt, um dem Betriebssystem die Einrichtung und Steuerung der einzelnen Hardware-Komponenten zu ermöglichen. ACPI löst sowohl Power-Management Plug and Play (PnP) als auch Advanced Power Management (APM) ab. Diese Schnittstelle bietet Informationen zu Akku, Netzteil, Temperatur, Ventilator und Systemereignissen wie „Deckel schließen“ oder „Akku-Ladezustand niedrig“.

Das BIOS bietet Tabellen mit Informationen zu den einzelnen Komponenten und Hardware-Zugriffsmethoden. Das Betriebssystem verwendet diese Informationen für Aufgaben wie das Zuweisen von Interrupts oder das Aktivieren bzw. Deaktivieren von Komponenten. Da das Betriebssystem die in BIOS gespeicherten Befehle ausführt, hängt die Funktionalität von der BIOS-Implementierung ab. Die Tabellen, die ACPI erkennen und laden kann, werden in `/var/log/boot.msg` gemeldet. Weitere Informationen zur Fehlersuche bei ACPI-Problemen finden Sie in Abschnitt 21.2.2, „Fehlersuche“ (S. 296).

21.2.1 Steuern der CPU-Leistung

Mit der CPU sind Energieeinsparungen auf drei verschiedene Weisen möglich:

- Frequenz- und Spannungsskalierung
- Drosseln der Taktfrequenz (T-Status)
- Versetzen des Prozessors in den Ruhezustand (C-Status)

Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden. Energiesparen bedeutet auch, dass sich das System weniger erhitzt und die Ventilatoren seltener in Betrieb sind.

Frequenzskalierung und Drosselung sind nur relevant, wenn der Prozessor belegt ist, da der sparsamste C-Zustand ohnehin gilt, wenn sich der Prozessor im Wartezustand befindet. Wenn die CPU belegt ist, ist die Frequenzskalierung die empfohlene Energiesparmethode. Häufig arbeitet der Prozessor nur im Teillast-Betrieb. In diesem Fall kann er mit einer niedrigeren Frequenz betrieben werden. Im Allgemeinen empfiehlt sich die dynamische Frequenzskalierung mit Steuerung durch den On-Demand-Governor im Kernel.

Drosselung sollte nur als letzter Ausweg verwendet werden, um die Betriebsdauer des Akkus trotz hoher Systemlast zu verlängern. Einige Systeme arbeiten bei zu hoher Drosselung jedoch nicht reibungslos. Außerdem hat die CPU-Drosselung keinen Sinn, wenn die CPU kaum ausgelastet ist.

Detaillierte Informationen hierzu finden Sie in Chapter 11, *Power Management* (↑*System Analysis and Tuning Guide*).

21.2.2 Fehlersuche

Es gibt zwei verschiedene Arten von Problemen. Einerseits kann der ACPI-Code des Kernel Fehler enthalten, die nicht rechtzeitig erkannt wurden. In diesem Fall wird eine Lösung zum Herunterladen bereitgestellt. Häufiger werden die Probleme vom BIOS verursacht. Manchmal werden Abweichungen von der ACPI-Spezifikation absichtlich in das BIOS integriert, um Fehler in der ACPI-Implementierung in anderen weit verbreiteten Betriebssystemen zu umgehen. Hardware-Komponenten, die ernsthafte Fehler in der ACPI-Implementierung aufweisen, sind in einer Blacklist festgehalten, die verhindert, dass der Linux-Kernel ACPI für die betreffenden Komponenten verwendet.

Der erste Schritt, der bei Problemen unternommen werden sollte, ist die Aktualisierung des BIOS. Wenn der Computer sich überhaupt nicht booten lässt, kann eventuell einer der folgenden Bootparameter Abhilfe schaffen:

pci=noacpi
: ACPI nicht zum Konfigurieren der PCI-Geräte verwenden.

acpi=ht
: Nur eine einfache Ressourcenkonfiguration durchführen. ACPI nicht für andere Zwecke verwenden.

acpi=off
: ACPI deaktivieren.

WARNUNG: Probleme beim Booten ohne ACPI

Einige neuere Computer (insbesondere SMP- und AMD64-Systeme) benötigen ACPI zur korrekten Konfiguration der Hardware. Bei diesen Computern kann die Deaktivierung von ACPI zu Problemen führen.

Manchmal ist der Computer durch Hardware gestört, die über USB oder FireWire angeschlossen ist. Wenn ein Computer nicht hochfährt, stecken Sie nicht benötigte Hardware aus und versuchen Sie es erneut.

Überwachen Sie nach dem Booten die Bootmeldungen des Systems mit dem Befehl `dmesg | grep -2i acpi` (oder überwachen Sie alle Meldungen, da das Problem möglicherweise nicht durch ACPI verursacht wurde). Wenn bei der Analyse einer ACPI-Tabelle ein Fehler auftritt, kann die wichtigste Tabelle – die DSDT (*Differentiated System Description Table*) – durch eine verbesserte Version ersetzt werden. In diesem

Fall wird die fehlerhafte DSDT des BIOS ignoriert. Das Verfahren wird in Abschnitt 21.4, „Fehlersuche“ (S. 299) erläutert.

In der Kernel-Konfiguration gibt es einen Schalter zur Aktivierung der ACPI-Fehlersuchmeldungen. Wenn ein Kernel mit ACPI-Fehlersuche kompiliert und installiert ist, werden detaillierte Informationen angezeigt.

Wenn Sie Probleme mit dem BIOS oder der Hardware feststellen, sollten Sie stets Kontakt mit den betreffenden Herstellern aufweisen. Insbesondere Hersteller, die nicht immer Hilfe für Linux anbieten, sollten mit den Problemen konfrontiert werden. Die Hersteller nehmen das Problem nur dann ernst, wenn sie feststellen, dass eine nennenswerte Zahl ihrer Kunden Linux verwendet.

21.2.2.1 Weiterführende Informationen

- `http://tldp.org/HOWTO/ACPI-HOWTO/` (detailliertes ACPI HOWTO, enthält DSDT-Patches)

- `http://www.acpi.info` (technische Daten zur Advanced Configuration & Power Interface)

- `http://www.lesswatts.org/projects/acpi/` (das ACPI4Linux-Projekt von Sourceforge)

- `http://acpi.sourceforge.net/dsdt/index.php` (DSDT-Patches von Bruno Ducrot)

21.3 Ruhezustand für Festplatte

In Linux kann die Festplatte vollständig ausgeschaltet werden, wenn sie nicht benötigt wird, oder sie kann in einem energiesparenderen oder ruhigeren Modus betrieben werden. Bei moderenen Notebooks müssen die Festplatten nicht manuell ausgeschaltet werden, da sie automatisch in einen Sparbetriebsmodus geschaltet werden, wenn sie nicht benötigt werden. Um die Energieeinsparungen zu maximieren, sollten Sie jedoch einige der folgenden Verfahren mit dem Kommando `hdparm` ausprobieren.

Hiermit können verschiedene Festplatteneinstellungen bearbeitet werden. Die Option `-y` schaltet die Festplatte sofort in den Stand-by-Modus. `-Y` versetzt sie in den Ruhe-

zustand. `hdparm -S x` führt dazu, dass die Festplatte nach einen bestimmten Inaktivitätszeitraum abgeschaltet wird. Ersetzen Sie *x* wie folgt: `0` deaktiviert diesen Mechanismus, sodass die Festplatte kontinuierlich ausgeführt wird. Werte von `1` bis `240` werden mit 5 Sekunden multipliziert. Werte von `241` bis `251` entsprechen 1- bis 11-mal 30 Minuten.

Die internen Energiesparoptionen der Festplatte lassen sich über die Option `-B` steuern. Wählen Sie einen Wert `0` (maximale Energieeinsparung) bis `255` (maximaler Durchsatz). Das Ergebnis hängt von der verwendeten Festplatte ab und ist schwer einzuschätzen. Die Geräuschentwicklung einer Festplatte können Sie mit der Option `-M` reduzieren. Wählen Sie einen Wert von `128` (ruhig) bis `254` (schnell).

Häufig ist es nicht so einfach, die Festplatte in den Ruhezustand zu versetzen. Bei Linux führen zahlreiche Prozesse Schreibvorgänge auf der Festplatte durch, wodurch diese wiederholt aus dem Ruhezustand reaktiviert wird. Daher sollten Sie unbedingt verstehen, wie Linux mit Daten umgeht, die auf die Festplatte geschrieben werden müssen. Zunächst werden alle Daten im RAM-Puffer gespeichert. Dieser Puffer wird vom `pdflush`-Daemon überwacht. Wenn die Daten ein bestimmtes Alter erreichen oder wenn der Puffer bis zu einem bestimmten Grad gefüllt ist, wird der Pufferinhalt auf die Festplatte übertragen. Die Puffergröße ist dynamisch und hängt von der Größe des Arbeitsspeichers und von der Systemlast ab. Standardmäßig werden für pdflush kurze Intervalle festgelegt, um maximale Datenintegrität zu erreichen. Das Programm überprüft den Puffer alle fünf Sekunden und schreibt die Daten auf die Festplatte. Die folgenden Variablen sind interessant:

`/proc/sys/vm/dirty_writeback_centisecs`
: Enthält die Verzögerung bis zur Reaktivierung eines pdflush-Threads (in Hundertstelsekunden).

`/proc/sys/vm/dirty_expire_centisecs`
: Definiert, nach welchem Zeitabschnitt eine schlechte Seite spätestens ausgeschrieben werden sollte. Der Standardwert ist `3000`, was 30 Sekunden bedeutet.

`/proc/sys/vm/dirty_background_ratio`
: Maximaler Prozentsatz an schlechten Seiten, bis pdflush damit beginnt, sie zu schreiben. Die Standardeinstellung ist `5` %.

/proc/sys/vm/dirty_ratio
: Wenn die schlechten Seiten diesen Prozentsatz des gesamten Arbeitsspeichers überschreiten, werden Prozesse gezwungen, während ihres Zeitabschnitts Puffer mit schlechten Seiten anstelle von weiteren Daten zu schreiben.

WARNUNG: Beeinträchtigung der Datenintegrität

Änderungen an den Einstellungen für den pdflush-Aktualisierungs-Daemon gefährden die Datenintegrität.

Abgesehen von diesen Prozessen schreiben protokollierende Journaling-Dateisysteme, wie Btrfs, Ext3, Ext4 und andere ihre Metadaten unabhängig von pdflush, was ebenfalls das Abschalten der Festplatte verhindert. Um dies zu vermeiden, wurde eine spezielle Kernel-Erweiterung für mobile Geräte entwickelt. Installieren Sie das laptop-mode-tools-Paket, und beachten Sie die Angaben in der Datei /usr/src/linux/Documentation/laptops/laptop-mode.txt.

Ein weiterer wichtiger Faktor ist die Art und Weise, wie sich die Programme verhalten. Gute Editoren beispielsweise schreiben regelmäßig verborgene Sicherungskopien der aktuell bearbeiteten Datei auf die Festplatte, wodurch die Festplatte wieder aktiviert wird. Derartige Funktionen können auf Kosten der Datenintegrität deaktiviert werden.

In dieser Verbindung verwendet der Mail-Daemon postfix die Variable POSTFIX_LAPTOP. Wenn diese Variable auf ja gesetzt wird, greift postfix wesentlich seltener auf die Festplatte zu.

In SUSE Linux Enterprise Desktop werden diese Technologien von Werkzeugen im Laptop-Modus gesteuert.

21.4 Fehlersuche

Alle Fehler- und Alarmmeldungen werden in der Datei /var/log/messages protokolliert. In den folgenden Abschnitten werden die häufigsten Probleme behandelt.

21.4.1 ACPI mit Hardware-Unterstützung aktiviert, bestimmte Funktionen sind jedoch nicht verfügbar

Falls Probleme mit ACPI auftreten, überprüfen Sie, ob die Ausgabe von `dmesg` ACPI-spezifische Meldungen enthält. Führen Sie hierzu das Kommando `dmesg|grep -i acpi` aus.

Zur Behebung des Problems kann eine BIOS-Aktualisierung erforderlich sein. Rufen Sie die Homepage Ihres Notebookherstellers auf, suchen Sie nach einer aktualisierten BIOS-Version und installieren Sie sie. Bitten Sie den Hersteller, die aktuellsten ACPI-Spezifikationen einzuhalten. Wenn der Fehler auch nach der BIOS-Aktualisierung noch besteht, gehen Sie wie folgt vor, um die fehlerhafte DSDT-Tabelle im BIOS mit einer aktualisierten DSDT zu ersetzen:

Prozedur 21.1 *Aktualisieren der DSDT-Tabelle im BIOS*

Für die nachstehende Prozedur müssen die folgenden Pakete installiert sein: `kernel-source`, `pmtools` und `mkinitrd`.

1. Laden Sie die DSDT für Ihr System von der Seite http://acpi.sourceforge.net/dsdt/index.php herunter. Prüfen Sie, ob die Datei dekomprimiert und kompiliert ist. Dies wird durch die Dateinamenserweiterung `.aml` (ACPI Machine Language) angezeigt. Wenn dies der Fall ist, fahren Sie mit Schritt 3 fort.

2. Wenn die heruntergeladene Tabelle stattdessen die Dateinamenserweiterung `.asl` (ACPI-Quellsprache) aufweist, kompilieren Sie sie mit dem folgenden Kommando:

   ```
   iasl -sa file.asl
   ```

3. Kopieren Sie die (resultierende) Datei `DSDT.aml` an einen beliebigen Speicherort (`/etc/DSDT.aml` wird empfohlen).

4. Bearbeiten Sie `/etc/sysconfig/kernel` und passen Sie den Pfad zur DSDT-Datei entsprechend an.

5 Starten Sie mkinitrd. Immer wenn Sie den Kernel installieren und mkinitrd verwenden, um eine initrd-Datei zu erstellen, wird die bearbeitete DSDT beim Booten des Systems integriert und geladen.

21.4.2 CPU-Frequenzsteuerung funktioniert nicht

Rufen Sie die Kernel-Quellen auf, um festzustellen, ob der verwendete Prozessor unterstützt wird. Möglicherweise ist ein spezielles Kernel-Modul bzw. eine Moduloption erforderlich, um die CPU-Frequenzsteuerung zu aktivieren. Wenn das kernel-source-Paket installiert ist, finden Sie diese Informationen unter /usr/src/linux/Documentation/cpu-freq/*.

21.4.3 Suspend und Stand-by funktionieren nicht

ACPI-Systeme können Probleme mit dem Stromspar- und Standby-Modus haben, wenn die DSDT-Implementierung (BIOS) fehlerhaft ist. Aktualisieren Sie in diesem Fall das BIOS.

Beim Versuch fehlerhafte Module zu entladen, reagiert das System nicht mehr oder das Suspend-Ereignis wird nicht ausgelöst. Dies kann auch dann passieren, wenn Sie keine Module entladen oder Dienste stoppen, die ein erfolgreiches Suspend-Ereignis verhindern. In beiden Fällen müssen Sie versuchen, das fehlerhafte Modul zu ermitteln, das den Energiesparmodus verhindert hat. Die Protokolldatei /var/log/pm-suspend.log enthält ausführliche Informationen über die einzelnen Vorgänge und mögliche Fehlerursachen. Ändern Sie die Variable SUSPEND_MODULES in /usr/lib/pm-utils/defaults, um problematische Module vor einem Suspend- oder Standby-Vorgang zu entladen.

21.5 Weiterführende Informationen

- http://en.opensuse.org/SDB:Suspend_to_RAM– Anleitung zur Einstellung von „Suspend to RAM“

- `http://old-en.opensuse.org/Pm-utils`– Anleitung zur Änderung des allgemeinen Suspend-Frameworks

22 Verwenden von Tablet PCs

SUSE® Linux Enterprise Desktop unterstützt auch Tablet-PCs. Sie erfahren im Folgenden, wie Sie Ihren Tablet PC installieren und konfigurieren. Außerdem werden Ihnen einige Linux*-Anwendungen vorgestellt, die die Eingabe über digitale Pens akzeptieren.

Die folgenden Tablet PCs werden unterstützt:

- Tablet PCs mit seriellem und USB Wacom Tablet (pen-basiert), Touchscreen- oder Multi-Touch-Geräte.
- Tablet PCs mit FinePoint-Geräten, z. B. Gateway C210X/M280E/CX2724 oder HP Compaq TC1000.
- Tablet PCs mit Touchscreen-Geräten, z. B. Asus R2H, Clevo TN120R, Fujitsu Siemens Computers P-Serie, LG C1, Samsung Q1/Q1-Ultra.

Nach der Installation der Tablet PC-Pakete und der Konfiguration Ihres Grafiktabletts können Sie Ihren Pen (auch als Stylus bezeichnet) für folgende Aktionen und Anwendungen verwenden:

- Anmelden bei KDM oder GDM
- Aufheben der Bildschirmsperre auf KDE- und GNOME-Desktops
- Aktionen, die auch durch andere Zeigegeräte (z. B. Maus oder Touch Pad) ausgelöst werden können, wie das Verschieben des Cursors auf dem Bildschirm, das Starten von Anwendungen, das Schließen, Skalieren und Verschieben von Fenstern, den Fokuswechsel in ein anderes Fenster oder das Ziehen und Ablegen von Objekten

- Verwenden der Bewegungserkennung in Anwendungen des X Window System
- Zeichnen mit GIMP
- Aufzeichnen von Notizen oder Skizzen mit Anwendungen wie Jarnal oder Xournal oder Bearbeiten größerer Textmengen mit Dasher

22.1 Installieren der Tablet PC-Pakete

Die für Tablet-PC benötigten Pakete sind im Installationsschema `TabletPC` enthalten. Wenn dieses Schema während der Installation ausgewählt wurde, sollten die folgenden Pakete bereits auf dem System installiert sein:

- `cellwriter`: Eine auf Zeichen basierende Kontrollleiste für handschriftliche Eingabe
- `jarnal`: Eine Java-basierte Anwendung für die Aufzeichnung von Notizen
- `xournal`: Eine Anwendung für die Aufzeichnung von Notizen und Skizzen
- `xstroke`: Ein Bewegungserkennungsprogramm für das X Window System
- `xvkbd`: Eine virtuelle Tastatur für das X Window System
- `x11-input-fujitsu`: Das X-Eingabemodul für Fujitsu P-Series-Tablets
- `x11-input-evtouch`: Das X-Eingabemodul für einige Tablet PCs mit Touchscreen
- `xorg-x11-driver-input`: Das X-Eingabemodul für Eingabegeräte, einschließlich des Moduls für Wacom-Geräte.

Falls diese Pakete noch nicht installiert sind, installieren Sie die erforderlichen Pakete manuell über die Kommandozeile oder wählen Sie das Schema `TabletPC` in YaST zur Installation aus.

22.2 Konfigurieren des Tablet-Geräts

Während der Installation wird Ihr Tablet oder Touch-Gerät standardmäßig konfiguriert. Falls Probleme mit der Konfiguration Ihres Wacom-Geräts auftreten, ändern Sie die Einstellungen mit dem Kommando `xsetwacom` in der Kommandozeile.

22.3 Verwenden der virtuellen Tastatur

Zur Anmeldung beim KDE- oder GNOME-Desktop oder zum Entsperren des Bildschirms können Sie Ihren Benutzernamen und Ihr Passwort wie gewohnt eingeben oder Sie können dazu die virtuelle Tastatur (xvkbd) verwenden, die sich unterhalb des Anmeldefelds befindet. Zur Konfiguration der Tastatur und zum Aufrufen der integrierten Hilfe klicken Sie links unten auf das Feld *xvkbd* und öffnen Sie das xvkbd-Hauptmenü.

Wenn Ihre Eingabe nicht sichtbar ist (oder nicht an das entsprechende Fenster übertragen wird), lenken Sie den Fokus um, indem Sie auf die *Fokus*-Taste in xvkbd und dann in das Fenster klicken, das die Tastaturereignisse empfangen soll.

Abbildung 22.1 *Virtuelle Tastatur von xvkbd*



Wenn Sie xvkbd nach der Anmeldung verwenden möchten, starten Sie es aus dem Hauptmenü oder über das Shell-Kommando `xvkbd`.

22.4 Drehen der Ansicht

Verwenden Sie KRandRTray (KDE) oder gnome-display-properties (GNOME), um Ihre Anzeige manuell interaktiv zu drehen oder die Größe zu verändern. Sowohl KRandRTray als auch gnome-display-properties sind Miniprogramme für die RANDR-Erweiterung von X Server.

Starten Sie KRandRTray oder gnome-display-properties im Hauptmenü oder geben Sie `krandrtray` oder `gnome-display-properties` ein, um das Miniprogramm von einer Shell aus zu starten. Nach dem Starten des Miniprogramms wird das Symbol für das Miniprogramm gewöhnlich zum Systemabschnitt der Kontrollleiste hinzugefügt. Wenn das gnome-display-properties-Symbol nicht automatisch im Systemabschnitt der Kontrollleiste angezeigt wird, stellen Sie sicher, dass *Symbole in Kontrollleisten anzeigen* im Dialogfeld *Einstellungen für Monitorauflösung* aktiviert ist.

Zum Drehen Ihrer Anzeige mit KRandRTray klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie *Anzeige konfigurieren*. Wählen Sie die gewünschte Ausrichtung im Konfigurations-Dialogfeld aus.

Zum Drehen Ihrer Anzeige mit gnome-display-properties klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie die gewünschte Ausrichtung aus. Die Ansicht wird sofort gedreht. Gleichzeitig ändert sich auch die Ausrichtung des Grafiktabletts. Es kann daher die Bewegungen des Pens nach wie vor richtig interpretieren.

Bei Problemen mit der Ausrichtung Ihres Desktops finden Sie weitere Informationen unter Abschnitt 22.7, „Fehlersuche“ (S. 311).

Weitere Informationen zu den desktopspezifischen Miniprogrammen für die RANDR-Erweiterung finden Sie unter Section “Monitor Settings” (Chapter 3, *Customizing Your Settings*, ↑*KDE User Guide*) und Abschnitt „Konfigurieren von Bildschirmen“ (Kapitel 3, *Anpassen Ihrer Einstellungen*, ↑*GNOME-Benutzerhandbuch*).

22.5 Verwenden der Bewegungserkennung

SUSE Linux Enterprise Desktop umfasst CellWriter und xstroke zur Bewegungserkennung. Beide Anwendungen akzeptieren Bewegungen mit dem Stift oder anderen Zeigegeräten als Eingabe für Anwendungen auf dem X Window System.

22.5.1 Verwenden von CellWriter

Mit CellWriter können Sie Zeichen in ein Zellraster schreiben; die Eingabe wird sofort auf Zeichenbasis erkannt. Nachdem Sie die Eingabe beendet haben, können Sie die Eingabe an die aktuell fokussierte Anwendung schicken. Bevor Sie CellWriter zur Bewegungserkennung nutzen können, muss die Anwendung zur Erkennung Ihrer Handschrift trainiert werden: Sie müssen jedes Zeichen anhand einer Zeichentabelle trainieren (nicht trainierte Zeichen werden nicht aktiviert und können daher nicht benutzt werden).

Prozedur 22.1 *Trainieren von CellWriter*

1 CellWriter starten Sie aus dem Hauptmenü oder von der Kommandozeile mit dem Kommando `cellwriter`. Beim ersten Start beginnt CellWriter automatisch im Trainingsmodus. Im Trainingsmodus wird ein Satz von Zeichen aus der aktuell ausgewählten Tastaturbelegung angezeigt.

2 Führen Sie die gewünschte Bewegung für ein Zeichen in der entsprechenden Zelle des Zeichens aus. Mit der ersten Eingabe ändert der Hintergrund seine Farbe in Weiß, während das Zeichen selbst in Hellgrau angezeigt wird. Wiederholen Sie die Bewegung mehrmals, bis das Zeichen in Schwarz angezeigt wird. Nicht trainierte Zeichen werden auf hellgrauem oder braunem Hintergrund (abhängig vom Farbschema auf dem Desktop) angezeigt.

3 Wiederholen Sie diesen Schritt, bis Sie CellWriter für alle benötigten Zeichen trainiert haben.

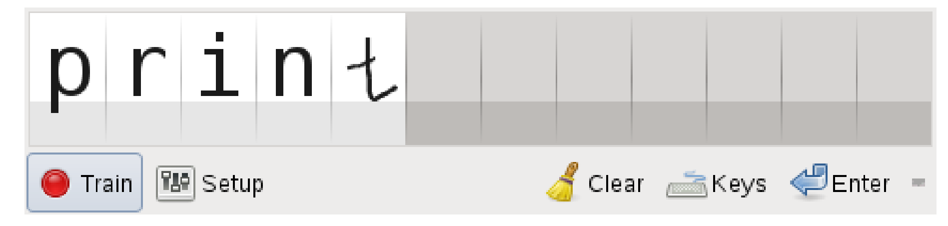
4 Wenn Sie CellWriter für eine andere Sprache trainieren möchten, klicken Sie auf die Schaltfläche *Setup* und wählen Sie eine Sprache in der Registerkarte *Sprachen* aus. *Schließen* Sie das Konfigurationsdialogfeld. Klicken Sie auf die Schaltfläche *Train* (Trainieren) und wählen Sie die Zeichentabelle aus dem Dropdown-Feld in

der unteren rechten Ecke des *CellWriter*-Fensters. Wiederholen Sie nun Ihr Training für die neue Zeichentabelle.

5 Nachdem Sie das Training für die Zeichentabelle abgeschlossen haben, klicken Sie auf die Schaltfläche *Train* (Trainieren), um in den normalen Modus zu wechseln.

Im normalen Modus zeigen die CellWriter-Fenster ein paar leere Zellen, in die die Bewegungen einzugeben sind. Die Zeichen werden erst dann an eine andere Anwendung gesendet, wenn Sie auf die Schaltfläche *Eingabe* klicken. Sie können also Zeichen korrigieren oder löschen, bevor Sie sie als Eingabe verwenden. Zeichen, die mit geringer Zuverlässigkeit erkannt wurden, werden markiert. Verwenden Sie zur Korrektur Ihrer Eingabe das Kontextmenü, das Sie öffnen, indem Sie mit der rechten Maustaste in eine Zelle klicken. Um ein Zeichen zu löschen, verwenden Sie entweder den Radierer Ihres Stifts oder klicken Sie mit der mittleren Maustaste, um die Zelle zu löschen. Wenn Ihre Eingabe in CellWriter beendet ist, definieren Sie die Anwendung, die die Eingabe empfangen soll, indem Sie in das Fenster der Anwendung klicken. Senden Sie dann die Eingabe an die Anwendung, indem Sie auf *Eingabe* klicken.

Abbildung 22.2 *Bewegungserkennung mit CellWriter*



Wenn Sie auf die Schaltfläche *Tasten* in CellWriter klicken, erhalten Sie eine virtuelle Tastastur, die Sie anstelle der Handschrifterkennung verwenden können.

Um CellWriter auszublenden, schließen Sie das CellWriter-Fenster. Die Anwendung erscheint nun als Symbol in Ihrem Systemabschnitt. Um das Eingabefenster erneut anzuzeigen, klicken Sie auf das Symbol im Systemabschnitt.

22.5.2 Verwenden von Xstroke

xstroke erkennt Bewegungen des Pens oder anderer Zeigegeräte als Eingabe für Anwendungen des X Window System. Das xstroke-Alphabet ist ein mit dem Graffiti*-Alphabet vergleichbares Unistroke-Alphabet. Wenn aktiviert, sendet xstroke die Eingabe an das Fenster, das aktuell den Fokus hält.

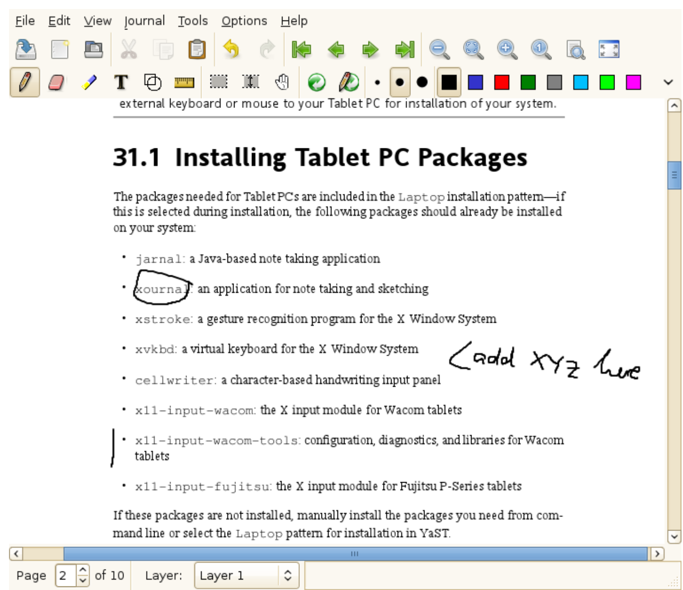
1. Starten Sie xstroke aus dem Hauptmenü oder über das Shell-Kommando `xstroke`. Dadurch wird dem Systemabschnitt der Kontrollleiste ein Bleistiftsymbol hinzugefügt.
2. Starten Sie die Anwendung, in die Sie mittels des Pens einen Text eingeben möchten (z. B. ein Terminalfenster, einen Texteditor oder einen LibreOffice.org Writer).
3. Zum Aktivieren der Bewegungserkennung klicken Sie einmal auf das Bleistiftsymbol.
4. Führen Sie auf dem Grafiktablett einige Bewegungen mit dem Pen oder einem anderen Zeigegerät aus. xstroke erfasst die Bewegungen und überträgt sie als Text in das fokussierte Anwendungsfenster.
5. Wenn Sie den Fokus in ein anderes Fenster wechseln möchten, klicken Sie mit dem Pen auf das betreffende Fenster und warten Sie einen Moment (oder verwenden Sie dazu das im Kontrollzentrum des Desktops festgelegte Tastenkürzel).
6. Zum Deaktivieren der Bewegungserkennung klicken Sie erneut auf das Bleistiftsymbol.

22.6 Aufzeichnen von Notizen und Skizzen mit dem Pen

Zum Anfertigen von Zeichnungen mit dem Pen können Sie einen professionellen Grafikeditor wie GIMP oder eine Notizenanwendung wie Xournal oder Jarnal verwenden. Sowohl mit Xournal als auch mit Jarnal können Sie mittels Pen Notizen aufzeichnen, Zeichnungen erstellen oder PDF-Dateien kommentieren. Die Java-basierte Anwendung Jarnal ist für verschiedene Plattformen verfügbar und bietet grundlegende Funktionen der Zusammenarbeit. Weitere Informationen hierzu finden Sie in `http://www.dklevine.com/general/software/tc1000/jarnal-net.htm`. Jarnal speichert den Inhalt in einem Archiv mit der Erweiterung .jaj. Dieses Archiv enthält auch eine Datei im SVG-Format.

Starten Sie Jarnal oder Xournal aus dem Hauptmenü oder über das Shell-Kommando `jarnal` bzw. `xournal`. Wenn Sie zum Beispiel in Xournal eine PDF-Datei kommentieren möchten, wählen Sie *Datei* > *PDF kommentieren* und öffnen Sie dann die PDF-Datei in Ihrem Dateisystem. Tragen Sie Ihre Kommentare mit dem Pen oder einem anderen Zeigegerät in die PDF-Datei ein und speichern Sie die Änderungen mit *File (Datei)* > *Export to PDF (Nach PDF exportieren)*.

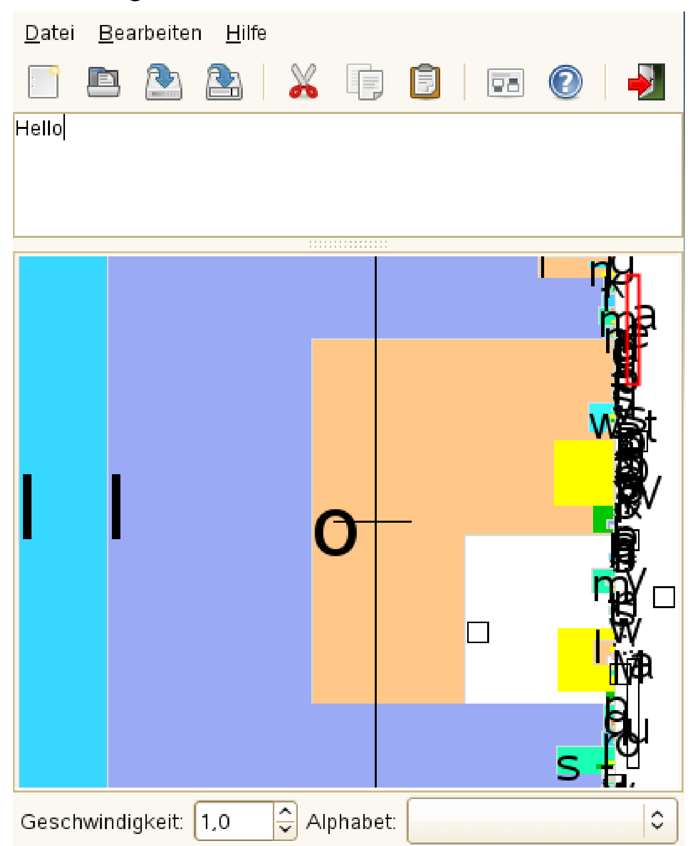
***Abbildung 22.3** Kommentieren einer PDF-Datei mit Xournal*



Dasher ist eine weitere nützliche Anwendung. Sie wurde speziell für Situationen entwickelt, in denen die Eingabe über die Tastatur unpraktisch oder unmöglich ist. Mit ein wenig Übung gelingt es recht bald, auch große Textmengen nur mit dem Pen (oder einem anderen Eingabegerät – selbst mit einem Eye Tracker) einzugeben.

Starten Sie Dasher aus dem Hauptmenü oder über das Shell-Kommando `dasher`. Sobald Sie den Pen in eine Richtung verschieben, beginnen die Buchstaben auf der rechten Seite vorbeizuzoomen. Aus den Buchstaben, die an dem Fadenkreuz in der Mitte vorbeilaufen, wird der Text erstellt bzw. vorausgesagt und im oberen Teil des Fensters angezeigt. Zum Beenden oder Starten der Texteingabe klicken Sie einmal mit dem Pen auf die Anzeige. Die Zoom-Geschwindigkeit können Sie unten im Fenster einstellen.

***Abbildung 22.4** Bearbeiten von Text mit Dasher*



Das Konzept von Dasher funktioniert in vielen Sprachen. Weitere Informationen finden Sie auf der Website von Dasher, auf der Sie eine umfassende Dokumentation, Demonstrationen und Schulungsdokumente vorfinden. Die Adresse der Website lautet `http://www.inference.phy.cam.ac.uk/dasher/`

22.7 Fehlersuche

Die virtuelle Tastatur wird im Anmeldefenster nicht angezeigt

Gelegentlich wird die virtuelle Tastatur im Anmeldefenster nicht angezeigt. Zur Behebung dieses Problems starten Sie X Server durch Drücken von Strg + Alt + <— neu bzw. drücken Sie die entsprechende Taste auf Ihrem Tablet PC (falls Sie

ein schlankes Modell ohne integrierte Tastatur verwenden). Wenn sich das Problem dadurch nicht beheben lässt, schließen Sie eine externe Tastatur an Ihr Modell an und melden Sie sich über diese Tastatur an.

Die Ausrichtung des Wacom-Grafiktabletts wird nicht geändert

Mit dem Kommando `xrandr` können Sie die Ausrichtung der Ansicht über eine Shell ändern. Geben Sie `xrandr --help` ein, um die verfügbaren Optionen dieses Kommandos anzuzeigen. Wenn Sie gleichzeitig die Ausrichtung des Grafiktabletts ändern möchten, müssen Sie das Kommando wie folgt eingeben:

- Normale Ausrichtung (Drehung um 0°):

  ```
  xrandr -o normal && xsetwacom --set "Serial Wacom Tablet" Rotate
  NONE
  ```

- Drehung um 90° (im Uhrzeigersinn, Hochformat):

  ```
  xrandr -o right && xsetwacom --set "Serial Wacom Tablet" Rotate CW
  ```

- Drehung um 180° (Querformat):

  ```
  xrandr -o inverted && xsetwacom --set "Serial Wacom Tablet" Rotate
  HALF
  ```

- Drehung um 270° (gegen den Uhrzeigersinn, Hochformat):

  ```
  xrandr -o left && xsetwacom set --"Serial Wacom Tablet" Rotate CCW
  ```

Die oben aufgeführten Kommandos hängen von der Ausgabe des Kommandos `xsetwacom list` ab. Ersetzen Sie „`Serial Wacom Tablet`“ mit der Ausgabe für den Stift oder das Touch-Gerät. Wenn Sie über ein Wacom-Gerät mit Touch-Unterstützung verfügen (Sie können den Cursor auf dem Tablet mit Ihren Fingern verschieben), müssen Sie das Touch-Gerät auch drehen.

22.8 Weiterführende Informationen

Einige der beschriebenen Anwendungen verfügen über keine integrierte Online-Hilfe. Informationen über deren Verwendung und Konfiguration finden Sie jedoch auf dem installierten System unter /usr/share/doc/package/*Paketname* bzw. im Web:

- Das Xournal-Handbuch finden Sie unter http://xournal.sourceforge.net/manual.html
- Die Jarnal-Dokumentation finden Sie unter http://jarnal.wikispaces.com/
- Die man-Seite zu xstroke finden Sie unter http://davesource.com/Projects/xstroke/xstroke.txt
- Eine HOWTO-Anleitung zur Konfiguration von X finden Sie auf der Linux Wacom-Website unter http://sourceforge.net/apps/mediawiki/linuxwacom/index.php?title=Configuring_X
- Eine überaus informative Website zum Dasher-Projekt finden Sie unter http://www.inference.phy.cam.ac.uk/dasher/
- Weitere Informationen und Dokumentation zu CellWriter finden Sie unter http://risujin.org/cellwriter/
- Informationen zu gnome-display-properties finden Sie in http://old-en.opensuse.org/GNOME/Multiscreen.



Teil IV. Services





23 Grundlegendes zu Netzwerken

Linux stellt die erforderlichen Netzwerkwerkzeuge und -funktionen für die Integration in alle Arten von Netzwerkstrukturen zur Verfügung. Der Netzwerkzugriff über eine Netzwerkkarte, ein Modem oder ein anderes Gerät kann mit YaST konfiguriert werden. Die manuelle Konfiguration ist ebenfalls möglich. In diesem Kapitel werden nur die grundlegenden Mechanismen und die relevanten Netzwerkkonfigurationsdateien behandelt.

Linux und andere Unix-Betriebssysteme verwenden das TCP/IP-Protokoll. Hierbei handelt es sich nicht um ein einzelnes Netzwerkprotokoll, sondern um eine Familie von Netzwerkprotokollen, die unterschiedliche Dienste zur Verfügung stellen. Die in Tabelle 23.1, „Verschiedene Protokolle aus der TCP/IP-Familie“ (S. 318) aufgelisteten Protokolle dienen dem Datenaustausch zwischen zwei Computern über TCP/IP. Über TCP/IP verbundene Netzwerke bilden zusammen ein weltweites Netzwerk, das auch als „das Internet“ bezeichnet wird.

RFC steht für *Bitte um Kommentare*. RFCs sind Dokumente, die unterschiedliche Internetprotokolle und Implementierungsverfahren für das Betriebssystem und seine Anwendungen beschreiben. Die RFC-Dokumente beschreiben das Einrichten der Internetprotokolle. Weitere Informationen zu diesen Protokollen finden Sie in den entsprechenden RFC-Dokumenten. Diese sind verfügbar unter `http://www.ietf.org/rfc.html`.

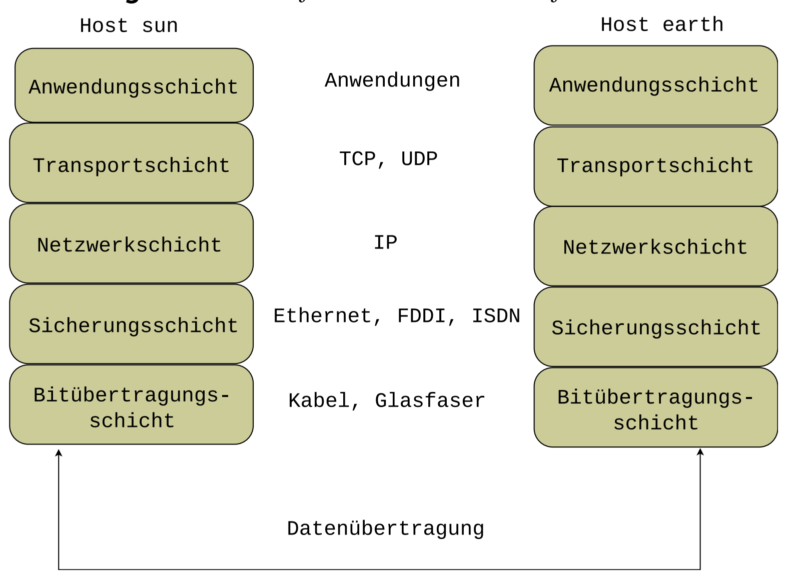
Tabelle 23.1 Verschiedene Protokolle aus der TCP/IP-Familie

Protokoll	Beschreibung
TCP	Transmission Control Protocol: Ein verbindungsorientiertes sicheres Protokoll. Die zu übertragenden Daten werden zuerst von der Anwendung als Datenstrom gesendet und vom Betriebssystem in das passende Format konvertiert. Die entsprechende Anwendung auf dem Zielhost empfängt die Daten im ursprünglichen Datenstromformat, in dem sie anfänglich gesendet wurden. TCP ermittelt, ob Daten bei der Übertragung verloren gegangen sind oder beschädigt wurden. TCP wird immer dann implementiert, wenn die Datensequenz eine Rolle spielt.
UDP	User Datagram Protocol: Ein verbindungsloses, nicht sicheres Protokoll. Die zu übertragenden Daten werden in Form von anwendungsseitig generierten Paketen gesendet. Es ist nicht garantiert, in welcher Reihenfolge die Daten beim Empfänger eingehen, und ein Datenverlust ist immer möglich. UDP ist geeignet für datensatzorientierte Anwendungen. Es verfügt über eine kürzere Latenzzeit als TCP.
ICMP	Internet Control Message Protocol: Dies ist im Wesentlichen kein Protokoll für den Endbenutzer, sondern ein spezielles Steuerungsprotokoll, das Fehlerberichte ausgibt und das Verhalten von Computern, die am TCP/IP-Datentrans-

Protokoll	Beschreibung
	fer teilnehmen, steuern kann. Außerdem bietet es einen speziellen Echomodus, der mit dem Programm „ping“ angezeigt werden kann.
IGMP	Internet Group Management Protocol: Dieses Protokoll kontrolliert das Verhalten des Rechners beim Implementieren von IP Multicast.

Der Datenaustausch findet wie in Abbildung 23.1, „Vereinfachtes Schichtmodell für TCP/IP“ (S. 319) dargestellt in unterschiedlichen Schichten statt. Die eigentliche Netzwerkschicht ist der unsichere Datentransfer über IP (Internet Protocol). Oberhalb von IP gewährleistet TCP (Transmission Control Protocol) bis zu einem gewissen Grad die Sicherheit des Datentransfers. Die IP-Schicht wird vom zugrunde liegenden Hardware-abhängigen Protokoll, z. B. Ethernet, unterstützt.

Abbildung 23.1 *Vereinfachtes Schichtmodell für TCP/IP*

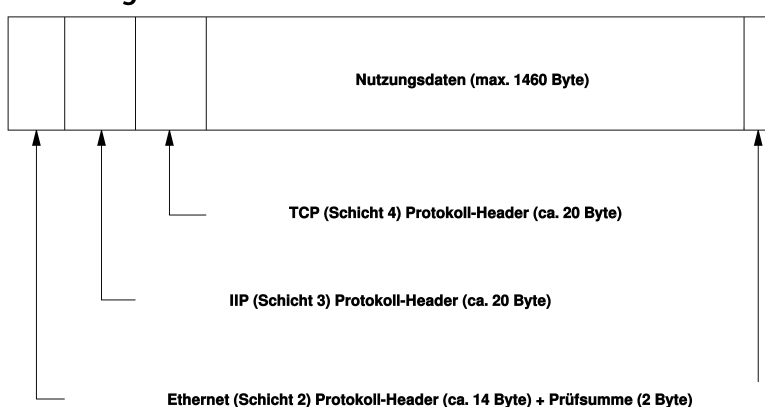


Dieses Diagramm bietet für jede Schicht ein oder zwei Beispiele. Die Schichten sind nach *Abstraktionsstufen* sortiert. Die unterste Schicht ist sehr Hardware-nah. Die oberste Schicht ist beinahe vollständig von der Hardware losgelöst. Jede Schicht hat ihre eigene spezielle Funktion. Die speziellen Funktionen der einzelnen Schichten gehen bereits aus ihrer Bezeichnung hervor. Die Datenverbindungs- und die physische Schicht repräsentieren das verwendete physische Netzwerk, z. B. das Ethernet.

Fast alle Hardwareprotokolle arbeiten auf einer paketorientierten Basis. Die zu übertragenden Daten werden in *Paketen* gesammelt (sie können nicht alle auf einmal gesendet werden). Die maximale Größe eines TCP/IP-Pakets beträgt ca. 64 KB. Die Pakete sind in der Regel jedoch sehr viel kleiner, da die Netzwerkhardware ein einschränkender Faktor sein kann. Die maximale Größe eines Datenpakets in einem Ethernet beträgt ca. 1500 Byte. Die Größe eines TCP/IP-Pakets ist auf diesen Wert begrenzt, wenn die Daten über ein Ethernet gesendet werden. Wenn mehr Daten übertragen werden, müssen vom Betriebssystem mehr Datenpakete gesendet werden.

Damit die Schichten ihre vorgesehenen Funktionen erfüllen können, müssen im Datenpaket zusätzliche Informationen über die einzelnen Schichten gespeichert sein. Diese Informationen werden im *Header* des Pakets gespeichert. Jede Schicht stellt jedem ausgehenden Paket einen kleinen Datenblock voran, den so genannten Protokoll-Header. Ein Beispiel für ein TCP/IP-Datenpaket, das über ein Ethernetkabel gesendet wird, ist in Abbildung 23.2, „TCP/IP-Ethernet-Paket“ (S. 320) dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

Abbildung 23.2 *TCP/IP-Ethernet-Paket*



Wenn eine Anwendung Daten über das Netzwerk sendet, werden diese Daten durch alle Schichten geleitet, die mit Ausnahme der physischen Schicht alle im Linux-Kernel implementiert sind. Jede Schicht ist für das Vorbereiten der Daten zur Weitergabe an die nächste Schicht verantwortlich. Die unterste Schicht ist letztendlich für das Senden der Daten verantwortlich. Bei eingehenden Daten erfolgt die gesamte Prozedur in umgekehrter Reihenfolge. Die Protokoll-Header werden von den transportierten Daten in den einzelnen Schichten wie die Schalen einer Zwiebel entfernt. Die Transportschicht ist schließlich dafür verantwortlich, die Daten den Anwendungen am Ziel zur Verfügung zu stellen. Auf diese Weise kommuniziert eine Schicht nur mit der direkt darüber bzw. darunter liegenden Schicht. Für Anwendungen ist es irrelevant, ob die Daten über ein 100 MBit/s schnelles FDDI-Netzwerk oder über eine 56-KBit/s-Modemleitung übertragen werden. Ähnlich spielt es für die Datenverbindung keine Rolle, welche Art von Daten übertragen wird, solange die Pakete das richtige Format haben.

23.1 IP-Adressen und Routing

Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf IPv4-Netzwerke. Informationen zum IPv6-Protokoll, dem Nachfolger von IPv4, finden Sie in Abschnitt 23.2, „IPv6 – Das Internet der nächsten Generation“ (S. 324).

23.1.1 IP-Adressen

Jeder Computer im Internet verfügt über eine eindeutige 32-Bit-Adresse. Diese 32 Bit (oder 4 Byte) werden in der Regel wie in der zweiten Zeile in Beispiel 23.1, „IP-Adressen schreiben“ (S. 321) dargestellt geschrieben.

Beispiel 23.1 *IP-Adressen schreiben*

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.     168.       0.      20
```

Im Dezimalformat werden die vier Byte in Dezimalzahlen geschrieben und durch Punkte getrennt. Die IP-Adresse wird einem Host oder einer Netzwerkschnittstelle zugewiesen. Sie kann weltweit nur einmal verwendet werden. Es gibt zwar Ausnahmen zu dieser Regel, diese sind jedoch für die folgenden Abschnitte nicht relevant.

Die Punkte in IP-Adressen geben das hierarchische System an. Bis in die 1990er-Jahre wurden IP-Adressen strikt in Klassen organisiert. Dieses System erwies sich jedoch als

zu wenig flexibel und wurde eingestellt. Heute wird das *klassenlose Routing* (CIDR, Classless Interdomain Routing) verwendet.

23.1.2 Netzmasken und Routing

Mit Netzmasken werden Adressräume eines Subnetzes definiert. Wenn sich in einem Subnetz zwei Hosts befinden, können diese direkt aufeinander zugreifen. Wenn sie sich nicht im selben Subnetz befinden, benötigen sie die Adresse eines Gateways, das den gesamten Verkehr für das Subnetz verarbeitet. Um zu prüfen, ob sich zwei IP-Adressen im selben Subnetz befinden, wird jede Adresse bitweise mit der Netzmaske „UND"-verknüpft. Sind die Ergebnisse identisch, befinden sich beide IP-Adressen im selben lokalen Netzwerk. Wenn unterschiedliche Ergebnisse ausgegeben werden, kann die entfernte IP-Adresse, und somit die entfernte Schnittstelle, nur über ein Gateway erreicht werden.

Weitere Informationen zur Funktionsweise von Netzmasken finden Sie in Beispiel 23.2, „Verknüpfung von IP-Adressen mit der Netzmaske" (S. 322). Die Netzmaske besteht aus 32 Bit, die festlegen, welcher Teil einer IP-Adresse zum Netzwerk gehört. Alle Bits mit dem Wert `1` kennzeichnen das entsprechende Bit in der IP-Adresse als zum Netzwerk gehörend. Alle Bits mit dem Wert `0` kennzeichnen Bits innerhalb des Subnetzes. Das bedeutet, je mehr Bits den Wert `1` haben, desto kleiner ist das Netzwerk. Da die Netzmaske immer aus mehreren aufeinander folgenden Bits mit dem Wert `1` besteht, ist es auch möglich, einfach die Anzahl der Bits in der Netzmaske zu zählen. In Beispiel 23.2, „Verknüpfung von IP-Adressen mit der Netzmaske" (S. 322) könnte das erste Netz mit 24 Bit auch als `192.168.0.0/24` geschrieben werden.

Beispiel 23.2 *Verknüpfung von IP-Adressen mit der Netzmaske*

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
---------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
---------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

Ein weiteres Beispiel: Alle Computer, die über dasselbe Ethernetkabel angeschlossen sind, befinden sich in der Regel im selben Subnetz und sind direkt zugreifbar. Selbst wenn das Subnetz physisch durch Switches oder Bridges unterteilt ist, können diese Hosts weiter direkt erreicht werden.

IP-Adressen außerhalb des lokalen Subnetzes können nur erreicht werden, wenn für das Zielnetzwerk ein Gateway konfiguriert ist. In den meisten Fällen wird der gesamte externe Verkehr über lediglich ein Gateway gehandhabt. Es ist jedoch auch möglich, für unterschiedliche Subnetze mehrere Gateways zu konfigurieren.

Wenn ein Gateway konfiguriert wurde, werden alle externen IP-Pakete an das entsprechende Gateway gesendet. Dieses Gateway versucht anschließend, die Pakete auf dieselbe Weise – von Host zu Host – weiterzuleiten, bis sie den Zielhost erreichen oder ihre TTL-Zeit (Time to Live) abgelaufen ist.

Tabelle 23.2 *Spezifische Adressen*

Adresstyp	Beschreibung
Netzwerkbasisadresse	Dies ist die Netzmaske, die durch UND mit einer Netzwerkadresse verknüpft ist, wie in Beispiel 23.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 322) unter `Result` dargestellt. Diese Adresse kann keinem Host zugewiesen werden.
Broadcast-Adresse	Dies bedeutet im Wesentlichen „Senden an alle Hosts in diesem Subnetz.“ Um die Broadcast-Adresse zu generieren, wird die Netzmaske in die binäre Form invertiert und mit einem logischen ODER mit der Netzwerkbasisadresse verknüpft. Das obige Beispiel ergibt daher die Adresse 192.168.0.255. Diese Adresse kann keinem Host zugeordnet werden.
Lokaler Host	Die Adresse `127.0.0.1` ist auf jedem Host dem „Loopback-Device“ zugewie-

Adresstyp	Beschreibung
	sen. Mit dieser Adresse und mit allen Adressen des vollständigen 127.0.0.0/8-Loopback-Netzwerks (wie bei IPv4 beschrieben) kann eine Verbindung zu Ihrem Computer eingerichtet werden. Bei IPv6 gibt es nur eine Loopback-Adresse (::1).

Da IP-Adressen weltweit eindeutig sein müssen, können Sie nicht einfach eine Adresse nach dem Zufallsprinzip wählen. Zum Einrichten eines privaten IP-basierten Netzwerks stehen drei Adressdomänen zur Verfügung. Diese können keine Verbindung zum Internet herstellen, da sie nicht über das Internet übertragen werden können. Diese Adressdomänen sind in RFC 1597 festgelegt und werden in Tabelle 23.3, „Private IP-Adressdomänen“ (S. 324) aufgelistet.

***Tabelle 23.3** Private IP-Adressdomänen*

Netzwerk/Netzmaske	Domäne
10.0.0.0/255.0.0.0	10.x.x.x
172.16.0.0/255.240.0.0	172.16.x.x – 172.31.x.x
192.168.0.0/255.255.0.0	192.168.x.x

23.2 IPv6 – Das Internet der nächsten Generation

Aufgrund der Entstehung des WWW (World Wide Web) hat das Internet in den letzten 15 Jahren ein explosives Wachstum mit einer immer größer werdenden Anzahl von Computern erfahren, die über TCP/IP kommunizieren. Seit Tim Berners-Lee bei CERN (http://public.web.cern.ch) 1990 das WWW erfunden hat, ist die Anzahl der Internethosts von ein paar tausend auf ca. 100 Millionen angewachsen.

Wie bereits erwähnt, besteht eine IPv4-Adresse nur aus 32 Bit. Außerdem gehen zahlreiche IP-Adressen verloren, da sie aufgrund der organisatorischen Bedingtheit der Netzwerke nicht verwendet werden können. Die Anzahl der in Ihrem Subnetz verfügbaren Adressen ist zwei hoch der Anzahl der Bits minus zwei. Ein Subnetz verfügt also beispielsweise über 2, 6 oder 14 Adressen. Um beispielsweise 128 Hosts mit dem Internet zu verbinden, benötigen Sie ein Subnetz mit 256 IP-Adressen, von denen nur 254 verwendbar sind, da zwei IP-Adressen für die Struktur des Subnetzes selbst benötigt werden: die Broadcast- und die Basisnetzwerkadresse.

Unter dem aktuellen IPv4-Protokoll sind DHCP oder NAT (Network Address Translation) die typischen Mechanismen, um einem potenziellen Adressmangel vorzubeugen. Kombiniert mit der Konvention, private und öffentliche Adressräume getrennt zu halten, können diese Methoden den Adressmangel sicherlich mäßigen. Das Problem liegt in der Konfiguration der Adressen, die schwierig einzurichten und zu verwalten ist. Um einen Host in einem IPv4-Netzwerk einzurichten, benötigen Sie mehrere Adressen, z. B. die IP-Adresse des Hosts, die Subnetzmaske, die Gateway-Adresse und möglicherweise die Adresse des Namenservers. Alle diese Einträge müssen bekannt sein und können nicht von anderer Stelle her abgeleitet werden.

Mit IPv6 gehören sowohl der Adressmangel als auch die komplizierte Konfiguration der Vergangenheit an. Die folgenden Abschnitte enthalten weitere Informationen zu den Verbesserungen und Vorteilen von IPv6 sowie zum Übergang vom alten zum neuen Protokoll.

23.2.1 Vorteile

Die wichtigste und augenfälligste Verbesserung durch das neue Protokoll ist der enorme Zuwachs des verfügbaren Adressraums. Eine IPv6-Adresse besteht aus 128-Bit-Werten und nicht aus den herkömmlichen 32 Bit. Dies ermöglicht mehrere Billiarden IP-Adressen.

IPv6-Adressen unterscheiden sich nicht nur hinsichtlich ihrer Länge gänzlich von ihren Vorgängern. Sie verfügen auch über eine andere interne Struktur, die spezifischere Informationen zu den Systemen und Netzwerken enthalten kann, zu denen sie gehören. Weitere Informationen hierzu finden Sie in Abschnitt 23.2.2, „Adresstypen und -struktur“ (S. 327).

In der folgenden Liste werden einige der wichtigsten Vorteile des neuen Protokolls aufgeführt:

Automatische Konfiguration

IPv6 macht das Netzwerk „Plug-and-Play“-fähig, d. h., ein neu eingerichtetes System wird ohne jegliche manuelle Konfiguration in das (lokale) Netzwerk integriert. Der neue Host verwendet die automatischen Konfigurationsmechanismen, um seine eigene Adresse aus den Informationen abzuleiten, die von den benachbarten Routern zur Verfügung gestellt werden. Dabei nutzt er ein Protokoll, das als *ND-Protokoll* (Neighbor Discovery) bezeichnet wird. Diese Methode erfordert kein Eingreifen des Administrators und für die Adresszuordnung muss kein zentraler Server verfügbar sein. Dies ist ein weiterer Vorteil gegenüber IPv4, bei dem für die automatische Adresszuordnung ein DHCP-Server erforderlich ist.

Wenn ein Router mit einem Switch verbunden ist, sollte der Router jedoch trotzdem periodische Anzeigen mit Flags senden, die den Hosts eines Netzwerks mitteilen, wie sie miteinander interagieren sollen. Weitere Informationen finden Sie im Artikel RFC 2462, auf der man-Seite `radvd.conf(5)` und im Artikel RFC 3315.

Mobilität

IPv6 ermöglicht es, einer Netzwerkschnittstelle gleichzeitig mehrere Adressen zuzuordnen. Benutzer können daher einfach auf mehrere Netzwerke zugreifen. Dies lässt sich mit den internationalen Roaming-Diensten vergleichen, die von Mobilfunkunternehmen angeboten werden: Wenn Sie das Mobilfunkgerät ins Ausland mitnehmen, meldet sich das Telefon automatisch bei einem ausländischen Dienst an, der sich im entsprechenden Bereich befindet. Sie können also überall unter der gleichen Nummer erreicht werden und können telefonieren als wären Sie zu Hause.

Sichere Kommunikation

Bei IPv4 ist die Netzwerksicherheit eine Zusatzfunktion. IPv6 umfasst IPSec als eine seiner Kernfunktionen und ermöglicht es Systemen, über einen sicheren Tunnel zu kommunizieren, um das Ausspionieren durch Außenstehende über das Internet zu verhindern.

Abwärtskompatibilität

Realistisch gesehen, ist es unmöglich, das gesamte Internet auf einmal von IPv4 auf IPv6 umzustellen. Daher ist es wichtig, dass beide Protokolle nicht nur im Internet, sondern auf einem System koexistieren können. Dies wird durch kompatible Adressen (IPv4-Adressen können problemlos in IPv6-Adressen konvertiert werden) und die Verwendung von Tunnels gewährleistet. Weitere Informationen hierzu finden Sie unter Abschnitt 23.2.3, „Koexistenz von IPv4 und IPv6“ (S. 332). Außerdem können Systeme eine *Dual-Stack-IP*-Technik verwenden, um beide

Protokolle gleichzeitig unterstützen zu können. Dies bedeutet, dass sie über zwei Netzwerk-Stacks verfügen, die vollständig unabhängig voneinander sind, sodass zwischen den beiden Protokollversionen keine Konflikte auftreten.

Bedarfsgerechte Dienste über Multicasting
: Mit IPv4 müssen einige Dienste, z. B. SMB, ihre Pakete via Broadcast an alle Hosts im lokalen Netzwerk verteilen. IPv6 erlaubt einen sehr viel feineren Ansatz, indem es Servern ermöglicht, Hosts über *Multicasting* anzusprechen, d. h. sie sprechen mehrere Hosts als Teile einer Gruppe an. Dies unterscheidet sich von der Adressierung aller Hosts über *Broadcasting* oder der Einzeladressierung der Hosts über *Unicasting*. Welche Hosts als Gruppe adressiert werden, kann je nach Anwendung unterschiedlich sein. Es gibt einige vordefinierte Gruppen, mit der beispielsweise alle Namenserver (die *Multicast-Gruppe „all name servers“*) oder alle Router (die *Multicast-Gruppe „all routers“*) angesprochen werden können.

23.2.2 Adresstypen und -struktur

Wie bereits erwähnt hat das aktuelle IP-Protokoll zwei wichtige Nachteile: Es stehen zunehmend weniger IP-Adressen zur Verfügung und das Konfigurieren des Netzwerks und Verwalten der Routing-Tabellen wird komplexer und aufwändiger. IPv6 löst das erste Problem durch die Erweiterung des Adressraums auf 128 Bit. Das zweite Problem wird durch die Einführung einer hierarchischen Adressstruktur behoben, die mit weiteren hoch entwickelten Techniken zum Zuordnen von Netzwerkadressen sowie mit dem *Multihoming* (der Fähigkeit, einem Gerät mehrere Adressen zuzuordnen und so den Zugriff auf mehrere Netzwerke zu ermöglichen) kombiniert wird.

Bei der Arbeit mit IPv6 ist es hilfreich, die drei unterschiedlichen Adresstypen zu kennen:

Unicast
: Adressen dieses Typs werden genau einer Netzwerkschnittstelle zugeordnet. Pakete mit derartigen Adressen werden nur einem Ziel zugestellt. Unicast-Adressen werden dementsprechend zum Übertragen von Paketen an einzelne Hosts im lokalen Netzwerk oder im Internet verwendet.

Multicast
: Adressen dieses Typs beziehen sich auf eine Gruppe von Netzwerkschnittstellen. Pakete mit derartigen Adressen werden an alle Ziele zugestellt, die dieser Gruppe angehören. Multicast-Adressen werden hauptsächlich von bestimmten Netzwerk-

diensten für die Kommunikation mit bestimmten Hostgruppen verwendet, wobei diese gezielt adressiert werden.

Anycast
: Adressen dieses Typs beziehen sich auf eine Gruppe von Schnittstellen. Pakete mit einer derartigen Adresse werden gemäß den Prinzipien des zugrunde liegenden Routing-Protokolls dem Mitglied der Gruppe gesendet, das dem Absender am nächsten ist. Anycast-Adressen werden verwendet, damit Hosts Informationen zu Servern schneller abrufen können, die im angegebenen Netzwerkbereich bestimmte Dienste anbieten. Sämtliche Server desselben Typs verfügen über dieselbe Anycast-Adresse. Wann immer ein Host einen Dienst anfordert, erhält er eine Antwort von dem vom Routing-Protokoll ermittelten nächstgelegenen Server. Wenn dieser Server aus irgendeinem Grund nicht erreichbar ist, wählt das Protokoll automatisch den zweitnächsten Server, dann den dritten usw. aus.

Eine IPv6-Adresse besteht aus acht vierstelligen Feldern, wobei jedes 16 Bit repräsentiert, und wird in hexadezimaler Notation geschrieben. Sie werden durch Doppelpunkte (`:`) getrennt. Alle führenden Null-Byte innerhalb eines bestimmten Felds können ausgelassen werden, alle anderen Nullen jedoch nicht. Eine weitere Konvention ist, dass mehr als vier aufeinander folgenden Null-Byte mit einem doppelten Doppelpunkt zusammengefasst werden können. Jedoch ist pro Adresse nur ein solcher doppelter Doppelpunkt (`::`) zulässig. Diese Art der Kurznotation wird in Beispiel 23.3, „Beispiel einer IPv6-Adresse" (S. 328) dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

Beispiel 23.3 *Beispiel einer IPv6-Adresse*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                           : 10 : 1000 : 1a4
```

Jeder Teil einer IPv6-Adresse hat eine festgelegte Funktion. Die ersten Byte bilden das Präfix und geben den Typ der Adresse an. Der mittlere Teil ist der Netzwerkteil der Adresse, der möglicherweise nicht verwendet wird. Das Ende der Adresse bildet der Hostteil. Bei IPv6 wird die Netzmaske definiert, indem die Länge des Präfixes nach einem Schrägstrich am Ende der Adresse angegeben wird. Adressen wie in Beispiel 23.4, „IPv6-Adressen mit Angabe der Präfix-Länge" (S. 329) enthalten Informationen zum Netzwerk (die ersten 64 Bit) und zum Hostteil (die letzten 64 Bit). Die `64` bedeutet, dass die Netzmaske mit 64 1-Bit-Werten von links gefüllt wird. Wie bei IPv4 wird die IP-Adresse mit den Werten aus der Netzmaske durch UND verknüpft, um zu ermitteln, ob sich der Host im selben oder einem anderen Subnetz befindet.

Beispiel 23.4 *IPv6-Adressen mit Angabe der Präfix-Länge*

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige von diesen sind in Tabelle 23.4, „Unterschiedliche IPv6-Präfixe“ (S. 329) aufgeführt.

Tabelle 23.4 *Unterschiedliche IPv6-Präfixe*

Präfix (hexadezimal)	Definition
`00`	IPv4-über-IPv6-Kompatibilitätsadressen. Diese werden zur Erhaltung der Kompatibilität mit IPv4 verwendet. Für diesen Adresstyp wird ein Router benötigt, der IPv6-Pakete in IPv4-Pakete konvertieren kann. Mehrere spezielle Adressen, z. B. die für das Loopback-Device, verfügen ebenfalls über dieses Präfix.
`2` oder `3` als erste Stelle	Aggregierbare globale Unicast-Adressen. Wie bei IPv4 kann eine Schnittstelle zugewiesen werden, um einen Teil eines bestimmten Subnetzes zu bilden. Aktuell stehen die folgenden Adressräume zur Verfügung: `2001::/16` (Adressraum Produktionsqualität) und `2002::/16` (6to4-Adressraum).
`fe80::/10`	Link-local-Adressen. Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.
`fec0::/10`	Site-local-Adressen. Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb des Organisationsnetzwerks, dem sie angehören. Damit entsprechen diese Adressen den bisherigen privaten Netzen (beispielsweise `10.x.x.x`).

Präfix (hexadezimal)	Definition
`ff`	Dies sind Multicast-Adressen.

Eine Unicast-Adresse besteht aus drei grundlegenden Komponenten:

Öffentliche Topologie
: Der erste Teil, der unter anderem auch eines der oben erwähnten Präfixe enthält, dient dem Routing des Pakets im öffentlichen Internet. Hier sind Informationen zum Provider oder der Institution kodiert, die den Netzwerkzugang bereitstellen.

Site-Topologie
: Der zweite Teil enthält Routing-Informationen zum Subnetz, in dem das Paket zugestellt werden soll.

Schnittstellen-ID
: Der dritte Teil identifiziert eindeutig die Schnittstelle, an die das Paket gerichtet ist. Dies erlaubt, die MAC-Adresse als Adressbestandteil zu verwenden. Da diese weltweit nur einmal vorhanden und zugleich vom Hardwarehersteller fest vorgegeben ist, vereinfacht sich die Konfiguration auf diese Weise sehr. Die ersten 64 Bit werden zu einem so genannten `EUI-64`-Token zusammengefasst. Dabei werden die letzten 48 Bit der MAC-Adresse entnommen und die restlichen 24 Bit enthalten spezielle Informationen, die etwas über den Typ des Tokens aussagen. Das ermöglicht dann auch, Geräten ohne MAC-Adresse (z. B. PPP- und ISDN-Verbindungen) ein `EUI-64`-Token zuzuweisen.

Abgeleitet aus diesem Grundaufbau werden bei IPv6 fünf verschiedene Typen von Unicast-Adressen unterschieden:

`::` (nicht spezifiziert)
: Diese Adresse verwendet ein Host als Quelladresse, wenn seine Netzwerkschnittstelle zum ersten Mal initialisiert wird und die Adresse noch nicht anderweitig ermittelt werden kann.

`::1` (Loopback)
: Adresse des Loopback-Device.

IPv4-kompatible Adressen

Die IPv6-Adresse setzt sich aus der IPv4-Adresse und einem Präfix von 96 0-Bits zusammen. Dieser Typ der Kompatibilitätsadresse wird beim Tunneling verwendet (siehe Abschnitt 23.2.3, „Koexistenz von IPv4 und IPv6“ (S. 332)). IPv4/IPv6-Hosts können so mit anderen kommunizieren, die sich in einer reinen IPv4-Umgebung befinden.

IPv6-gemappte IPv4-Adressen

Dieser Adresstyp gibt die Adresse in IPv6-Notation an.

Lokale Adressen

Es gibt zwei Typen von Adressen zum rein lokalen Gebrauch:

link-local

Dieser Adresstyp ist ausschließlich für den Gebrauch im lokalen Subnetz bestimmt. Router dürfen Pakete mit solcher Ziel- oder Quelladresse nicht an das Internet oder andere Subnetze weiterreichen. Diese Adressen zeichnen sich durch ein spezielles Präfix (`fe80::/10`) und die Schnittstellen-ID der Netzwerkkarte aus. Der Mittelteil der Adresse besteht aus Null-Bytes. Diese Art Adresse wird von den Autokonfigurationsmethoden verwendet, um Hosts im selben Subnetz anzusprechen.

site-local

Pakete mit diesem Adresstyp werden an andere Subnetze weitergleitet, müssen jedoch innerhalb des firmeneigenen Netzwerks verbleiben. Solche Adressen werden für Intranets eingesetzt und sind ein Äquivalent zu den privaten IPv4-Adressen. Neben einem definierten Präfix (`fec0::/10`) und der Schnittstellen-ID enthalten diese Adressen ein 16-Bit-Feld, in dem die Subnetz-ID kodiert ist. Der Rest wird wieder mit Null-Bytes aufgefüllt.

Zusätzlich gibt es in IPv6 eine grundsätzlich neue Funktion: Einer Netzwerkschnittstelle werden üblicherweise mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netze zur Verfügung stehen. Eines dieser Netzwerke kann mit der MAC-Adresse und einem bekannten Präfix vollautomatisch konfiguriert werden, sodass sofort nach der Aktivierung von IPv6 alle Hosts im lokalen Netz über Link-local-Adressen erreichbar sind. Durch die MAC-Adresse als Bestandteil der IP-Adresse ist jede dieser Adressen global eindeutig. Einzig die Teile der *Site-Topologie* und der *öffentlichen Topologie* können variieren, je nachdem in welchem Netz dieser Host aktuell zu erreichen ist.

Bewegt sich ein Host zwischen mehreren Netzen hin und her, braucht er mindestens zwei Adressen. Die eine, seine *Home-Adresse*, beinhaltet neben der Schnittstellen-ID die Informationen zu dem Heimatnetz, in dem der Computer normalerweise betrieben wird, und das entsprechende Präfix. Die Home-Adresse ist statisch und wird in der Regel nicht verändert. Alle Pakete, die für diesen Host bestimmt sind, werden ihm sowohl im eigenen als auch in fremden Netzen zugestellt. Möglich wird die Zustellung im Fremdnetz über wesentliche Neuerungen des IPv6-Protokolls, z. B. *Stateless Autoconfiguration* und *Neighbor Discovery*. Der mobile Rechner hat neben seiner Home-Adresse eine oder mehrere weitere Adressen, die zu den fremden Netzen gehören, in denen er sich bewegt. Diese Adressen heißen *Care-of*-Adressen. Im Heimatnetz des mobilen Rechners muss eine Instanz vorhanden sein, die an seine Home-Adresse gerichtete Pakete nachsendet, sollte er sich in einem anderen Netz befinden. Diese Funktion wird in einer IPv6-Umgebung vom *Home-Agenten* übernommen. Er stellt alle Pakete, die an die Home-Adresse des mobilen Rechners gerichtet sind, über einen Tunnel zu. Pakete, die als Zieladresse die Care-of-Adresse tragen, können ohne Umweg über den Home-Agenten zugestellt werden.

23.2.3 Koexistenz von IPv4 und IPv6

Die Migration aller mit dem Internet verbundenen Hosts von IPv4 auf IPv6 wird nicht auf einen Schlag geschehen. Vielmehr werden das alte und das neue Protokoll noch eine ganze Weile nebeneinanderher existieren. Die Koexistenz auf einem Rechner ist dann möglich, wenn beide Protokolle im *Dual Stack*-Verfahren implementiert sind. Es bleibt aber die Frage, wie IPv6-Rechner mit IPv4-Rechnern kommunizieren können und wie IPv6-Pakete über die momentan noch vorherrschenden IPv4-Netze transportiert werden sollen. Tunneling und die Verwendung von Kompatibilitätsadressen (siehe Abschnitt 23.2.2, „Adresstypen und -struktur“ (S. 327)) sind hier die besten Lösungen.

IPv6-Hosts, die im (weltweiten) IPv4-Netzwerk mehr oder weniger isoliert sind, können über Tunnel kommunizieren: IPv6-Pakete werden als IPv4-Pakete gekapselt und so durch ein ein IPv4-Netzwerk übertragen. Ein *Tunnel* ist definiert als die Verbindung zwischen zwei IPv4-Endpunkten. Hierbei müssen die Pakete die IPv6-Zieladresse (oder das entsprechende Präfix) und die IPv4-Adresse des entfernten Hosts am Tunnelendpunkt enthalten. Einfache Tunnel können von den Administratoren zwischen ihren Netzwerken manuell und nach Absprache konfiguriert werden. Ein solches Tunneling wird *statisches Tunneling* genannt.

Trotzdem reicht manuelles Tunneling oft nicht aus, um die Menge der zum täglichen vernetzten Arbeiten nötigen Tunnel aufzubauen und zu verwalten. Aus diesem Grund

wurden für IPv6 drei verschiedene Verfahren entwickelt, die das *dynamische Tunneling* erlauben:

6over4
: IPv6-Pakete werden automatisch in IPv4-Pakete verpackt und über ein IPv4-Netzwerk versandt, in dem Multicasting aktiviert ist. IPv6 wird vorgespiegelt, das gesamte Netzwerk (Internet) sei ein einziges, riesiges LAN (Local Area Network). So wird der IPv4-Endpunkt des Tunnel automatisch ermittelt. Nachteile dieser Methode sind die schlechte Skalierbarkeit und die Tatsache, dass IP-Multicasting keineswegs im gesamten Internet verfügbar ist. Diese Lösung eignet sich für kleinere Netzwerke, die die Möglichkeit von IP-Multicasting bieten. Die zugrunde liegenden Spezifikationen sind in RFC 2529 enthalten.

6to4
: Bei dieser Methode werden automatisch IPv4-Adressen aus IPv6-Adressen generiert. So können isolierte IPv6-Hosts über ein IPv4-Netz miteinander kommunizieren. Allerdings gibt es einige Probleme, die die Kommunikation zwischen den isolierten IPv6-Hosts und dem Internet betreffen. Diese Methode wird in RFC 3056 beschrieben.

IPv6 Tunnel Broker
: Dieser Ansatz sieht spezielle Server vor, die für IPv6 automatisch dedizierte Tunnel anlegen. Diese Methode wird in RFC 3053 beschrieben.

23.2.4 IPv6 konfigurieren

Um IPv6 zu konfigurieren, müssen Sie auf den einzelnen Arbeitsstationen in der Regel keine Änderungen vornehmen. IPv6 ist standardmäßig aktiviert. Sie können IPv6 während der Installation im Schritt der Netzwerkkonfiguration deaktivieren (siehe Abschnitt „Netzwerkkonfiguration“ (Kapitel 3, *Installation mit YaST*, ↑*Bereitstellungshandbuch*)). Um IPv6 auf einem installierten System zu deaktivieren oder zu aktivieren, verwenden Sie das Modul YaST-*Netzwerkeinstellungen*. Aktivieren oder deaktivieren Sie auf dem Karteireiter *Globale Optionen* die Option *IPv6 aktivieren*, falls nötig. Wenn Sie es bis zum nächsten Neustart vorübergehend aktivieren möchten, geben Sie `modprobe -i ipv6` als `root` ein. Es ist grundsätzlich unmöglich, das ipv6-Modul zu entladen, nachdem es geladen wurde.

Aufgrund des Konzepts der automatischen Konfiguration von IPv6 wird der Netzwerkkarte eine Adresse im *Link-local*-Netzwerk zugewiesen. In der Regel werden Routing-

Tabellen nicht auf Arbeitsstationen verwaltet. Bei Netzwerkroutern kann von der Arbeitsstation unter Verwendung des *Router-Advertisement-Protokolls* abgefragt werden, welches Präfix und welche Gateways implementiert werden sollen. Zum Einrichten eines IPv6-Routers kann das radvd-Programm verwendet werden. Dieses Programm informiert die Arbeitsstationen darüber, welches Präfix und welche Router für die IPv6-Adressen verwendet werden sollen. Alternativ können Sie die Adressen und das Routing auch mit zebra/quagga automatisch konfigurieren.

Weitere Informationen zum Einrichten der unterschiedlichen Tunneltypen mithilfe der Dateien im Verzeichnis `/etc/sysconfig/network` finden Sie auf der man-Seite „ifcfg-tunnel (5)“.

23.2.5 Weiterführende Informationen

Das komplexe IPv6-Konzept wird im obigen Überblick nicht vollständig abgedeckt. Weitere ausführliche Informationen zu dem neuen Protokoll finden Sie in den folgenden Online-Dokumentationen und -Büchern:

`http://www.ipv6.org/`
: Alles rund um IPv6.

`http://www.ipv6day.org`
: Alle Informationen, die Sie benötigen, um Ihr eigenes IPv6-Netzwerk zu starten.

`http://www.ipv6-to-standard.org/`
: Die Liste der IPv6-fähigen Produkte.

`http://www.bieringer.de/linux/IPv6/`
: Hier finden Sie den Beitrag „Linux IPv6 HOWTO“ und viele verwandte Links zum Thema.

RFC 2640
: Die grundlegenden IPv6-Spezifikationen.

IPv6 Essentials
: Ein Buch, in dem alle wichtigen Aspekte zum Thema enthalten sind, ist *IPv6 Essentials* von Silvia Hagen (ISBN 0-596-00125-8).

23.3 Namensauflösung

Mithilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden und umgekehrt auch ein Name einer IP-Adresse. Unter Linux erfolgt diese Umwandlung üblicherweise durch eine spezielle Software namens bind. Der Computer, der diese Umwandlung dann erledigt, nennt sich *Namenserver*. Dabei bilden die Namen wieder ein hierarchisches System, in dem die einzelnen Namensbestandteile durch Punkte getrennt sind. Die Namenshierarchie ist aber unabhängig von der oben beschriebenen Hierarchie der IP-Adressen.

Ein Beispiel für einen vollständigen Namen wäre `jupiter.example.com`, geschrieben im Format `Hostname.Domäne`. Ein vollständiger Name, der als *Fully Qualified Domain Name* oder kurz als FQDN bezeichnet wird, besteht aus einem Host- und einem Domänennamen (`example.com`). Ein Bestandteil des Domänennamens ist die *Top Level Domain* oder TLD (`com`).

Aus historischen Gründen ist die Zuteilung der TLDs etwas verwirrend. So werden in den USA traditionell dreibuchstabige TLDs verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen. Seit 2000 stehen zusätzliche TLDs für spezielle Sachgebiete mit zum Teil mehr als drei Buchstaben zur Verfügung (z. B. `.info`, `.name`, `.museum`).

In der Frühzeit des Internets (vor 1990) gab es die Datei`/etc/hosts`, in der die Namen aller im Internet vertretenen Rechner gespeichert waren. Dies erwies sich bei der schnell wachsenden Menge der mit dem Internet verbundenen Computer als unpraktikabel. Deshalb wurde eine dezentralisierte Datenbank entworfen, die die Hostnamen verteilt speichern kann. Diese Datenbank, eben jener oben erwähnte Namenserver, hält also nicht die Daten aller Computer im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere Namenserver weiterdelegieren.

An der Spitze der Hierarchie befinden sich die *Root-Namenserver*. Die root-Namenserver verwalten die Domänen der obersten Ebene (Top Level Domains) und werden vom Network Information Center (NIC) verwaltet. Der Root-Namenserver kennt die jeweils für eine Top Level Domain zuständigen Namenserver. Weitere Informationen zu TLD-NICs finden Sie unter `http://www.internic.net`.

DNS kann noch mehr als nur Hostnamen auflösen. Der Namenserver weiß auch, welcher Host für eine ganze Domäne E-Mails annimmt, der so genannte *Mail Exchanger (MX)*.

Damit auch Ihr Rechner einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Namenserver mit einer IP-Adresse bekannt sein. Die Konfiguration eines Namenservers erledigen Sie komfortabel mithilfe von YaST. Falls Sie eine Einwahl über Modem vornehmen, kann es sein, dass die manuelle Konfiguration eines Namenservers nicht erforderlich ist. Das Einwahlprotokoll liefert die Adresse des Namenservers bei der Einwahl gleich mit.

Eng verwandt mit DNS ist das Protokoll `whois`. Mit dem gleichnamigen Programm whois können Sie schnell ermitteln, wer für eine bestimmte Domäne verantwortlich ist.

ANMERKUNG: MDNS- und .local-Domänennamen

Die Domäne `.local` der obersten Stufe wird vom Resolver als link-local-Domäne behandelt. DNS-Anforderungen werden als Multicast-DNS-Anforderungen anstelle von normalen DNS-Anforderungen gesendet. Wenn Sie in Ihrer Nameserver-Konfiguration die Domäne `.local` verwenden, müssen Sie diese Option in `/etc/host.conf` ausschalten. Weitere Informationen finden Sie auf der man-Seite `host.conf`.

Wenn Sie MDNS während der Installation ausschalten möchten, verwenden Sie `nomdns=1` als Boot-Parameter.

Weitere Informationen zum Multicast-DNS finden Sie unter `http://www.multicastdns.org`.

23.4 Konfigurieren von Netzwerkverbindungen mit YaST

Unter Linux gibt es viele unterstützte Netzwerktypen. Die meisten verwenden unterschiedliche Gerätenamen und die Konfigurationsdateien sind im Dateisystem an unterschiedlichen Speicherorten verteilt. Einen detaillierten Überblick über die Aspekte der manuellen Netzwerkkonfiguration finden Sie in Abschnitt 23.6, „Manuelle Netzwerkkonfiguration“ (S. 362).

In SUSE Linux Enterprise Desktop mit standardmäßig aktivem NetworkManager sind alle Netzwerkkarten konfiguriert. Wenn NetworkManager nicht aktiv ist, wird nur die erste Schnittstelle mit Link-Up (einem angeschlossenen Netzwerkkabel) automatisch konfiguriert. Zusätzliche Hardware kann jederzeit nach Abschluss der Installation auf dem installierten System konfiguriert werden. In den folgenden Abschnitten wird die Netzwerkkonfiguration für alle von SUSE Linux Enterprise Desktop unterstützten Netzwerkverbindungen beschrieben.

23.4.1 Konfigurieren der Netzwerkkarte mit YaST

Zur Konfiguration verkabelter oder drahtloser Netzwerkkarten in YaST wählen Sie *Netzwerkgeräte* > *Netzwerkeinstellungen*. Nach dem Öffnen des Moduls zeigt YaST das Dialogfeld *Netzwerkeinstellungen* mit den vier Karteireitern *Globale Optionen*, *Übersicht*, *Hostname/DNS* und *Routing* an.

Auf dem Karteireiter *Globale Optionen* können allgemeine Netzwerkoptionen wie die Verwendung der Optionen NetworkManager, IPv6 und allgemeine DHCP-Optionen festgelegt werden. Weitere Informationen finden Sie unter Abschnitt 23.4.1.1, „Konfigurieren globaler Netzwerkoptionen“ (S. 338).

Der Karteireiter *Übersicht* enthält Informationen über installierte Netzwerkschnittstellen und -konfigurationen. Jede korrekt erkannte Netzwerkkarte wird dort mit ihrem Namen aufgelistet. In diesem Dialogfeld können Sie Karten manuell konfigurieren, entfernen oder ihre Konfiguration ändern. Informationen zum manuellen Konfigurieren von Karten, die nicht automatisch erkannt wurden, finden Sie unter Abschnitt 23.4.1.3, „Konfigurieren einer unerkannten Netzwerkkarte“ (S. 346). Informationen zum Ändern

der Konfiguration einer bereits konfigurierten Karte finden Sie unter Abschnitt 23.4.1.2, „Ändern der Konfiguration einer Netzwerkkarte“ (S. 340).

Auf dem Karteireiter *Hostname/DNS* können der Hostname des Computers sowie die zu verwendenden Nameserver festgelegt werden. Weitere Informationen finden Sie unter Abschnitt 23.4.1.4, „Konfigurieren des Hostnamens und DNS“ (S. 347).

Der Karteireiter *Routing* wird zur Konfiguration des Routings verwendet. Weitere Informationen finden Sie unter Abschnitt 23.4.1.5, „Konfigurieren des Routings“ (S. 349).

Abbildung 23.3 *Konfigurieren der Netzwerkeinstellungen*



23.4.1.1 Konfigurieren globaler Netzwerkoptionen

Auf dem Karteireiter *Globale Optionen* des YaST-Moduls *Netzwerkeinstellungen* können wichtige globale Netzwerkoptionen wie die Verwendung der Optionen Network-Manager, IPv6 und DHCP-Client festgelegt werden. Diese Einstellungen sind für alle Netzwerkschnittstellen anwendbar.

Unter *Netzwerkeinrichtungsmethode* wählen Sie die Methode aus, mit der Netzwerkverbindungen verwaltet werden sollen. Wenn die Verbindungen für alle Schnittstellen über das Desktop-Applet NetworkManager verwaltet werden sollen, wählen Sie *Benutzergesteuert mithilfe von NetworkManager* aus. Diese Option eignet sich besonders für den Wechsel zwischen verschiedenen verkabelten und drahtlosen Netzwerken. Wenn Sie keine Desktop-Umgebung (GNOME oder KDE) ausführen oder wenn Ihr Computer ein Xen-Server oder ein virtuelles System ist oder Netzwerkdienste wie DHCP oder DNS in Ihrem Netzwerk zur Verfügung stellt, verwenden Sie die *Traditionelle Methode mit ifup*. Beim Einsatz von NetworkManager sollte `nm-applet` verwendet werden, um Netzwerkoptionen zu konfigurieren. Die Karteireiter *Übersicht*, *Hostname/DNS* und *Routing* des Moduls *Netzwerkeinstellungen* sind dann deaktiviert. Weitere Informationen zu NetworkManager finden Sie in Kapitel 26, *Verwendung von NetworkManager* (S. 399).

Geben Sie unter *IPv6 Protocol Settings* (IPv6-Protokolleinstellungen) an, ob Sie das IPv6-Protokoll verwenden möchten. IPv6 kann parallel zu IPv4 verwendet werden. IPv6 ist standardmäßig aktiviert. In Netzwerken, die das IPv6-Protokoll nicht verwenden, können die Antwortzeiten jedoch schneller sein, wenn dieses Protokoll deaktiviert ist. Zum Deaktivieren von IPv6 deaktivieren Sie die Option *IPv6 aktivieren*. Dadurch wird das automatische Laden des Kernel-Moduls von IPv6 unterbunden. Die Einstellungen werden nach einem Neustart übernommen.

Unter *Optionen für DHCP-Client* konfigurieren Sie die Optionen für den DHCP-Client. Wenn der DHCP-Client den Server anweisen soll, seine Antworten immer per Broadcast zu versenden, aktivieren Sie *Broadcast-Antwort anfordern*. Diese Einstellung ist vermutlich erforderlich, wenn Sie Ihren Computer in verschiedenen Netzwerken verwenden. Die *Kennung für DHCP-Client* muss innerhalb eines Netzwerks für jeden DHCP-Client eindeutig sein. Wenn dieses Feld leer bleibt, wird standardmäßig die Hardware-Adresse der Netzwerkschnittstelle als Kennung übernommen. Falls Sie allerdings mehrere virtuelle Computer mit der gleichen Netzwerkschnittstelle und damit der gleichen Hardware-Adresse ausführen, sollten Sie hier eine eindeutige Kennung in beliebigem Format eingeben.

Unter *Zu sendender Hostname* wird eine Zeichenkette angegeben, die für das Optionsfeld „Hostname" verwendet wird, wenn dhcpcd Nachrichten an den DHCP-Server sendet. Einige DHCP-Server aktualisieren Namenserver-Zonen gemäß diesem Hostnamen (dynamischer DNS). Bei einigen DHCP-Servern muss das Optionsfeld *Zu sendender Hostname* in den DHCP-Nachrichten der Clients zudem eine bestimmte Zeichenkette enthalten. Übernehmen Sie die Einstellung `AUTO`, um den aktuellen Hostnamen zu senden (d. h. der aktuelle in `/etc/HOSTNAME` festgelegte Hostname). Lassen Sie das

Optionsfeld leer, wenn kein Hostname gesendet werden soll. Wenn die Standardroute nicht gemäß der Informationen von DHCP geändert werden soll, deaktivieren Sie *Standardroute über DHCP ändern*.

23.4.1.2 Ändern der Konfiguration einer Netzwerkkarte

Wenn Sie die Konfiguration einer Netzwerkkarte ändern möchten, wählen Sie die Karte aus der Liste der erkannten Karten unter *Netzwerkeinstellungen* > *Übersicht* in YaST aus, und klicken Sie auf *Bearbeiten*. Das Dialogfeld *Netzwerkkarten-Setup* wird angezeigt. Hier können Sie die Kartenkonfiguration auf den Karteireitern *Allgemein*, *Adresse* und *Hardware* anpassen. Genauere Informationen zur drahtlosen Kartenkonfiguration finden Sie unter Abschnitt 20.5, „Konfiguration mit YaST" (S. 278).

IP-Adressen konfigurieren

Die IP-Adresse der Netzwerkkarte oder die Art der Festlegung dieser IP-Adresse kann auf dem Karteireiter *Adresse* im Dialogfeld *Einrichten der Netzwerkkarte* festgelegt werden. Die Adressen IPv4 und IPv6 werden unterstützt. Für die Netzwerkkarte können die Einstellungen *Keine IP-Adresse* (nützlich für eingebundene Geräte), *Statisch zugewiesene IP-Adresse* (IPv4 oder IPv6) oder *Dynamische Adresse* über *DHCP* und/oder *Zeroconf* zugewiesen werden.

Wenn Sie *Dynamische Adresse* verwenden, wählen Sie, ob *Nue DHCP-Version 4* (für IPv4), *Nur DHCP-Version 6* (für IPv6) oder *DHCP-Version 4 und 6* verwendet werden soll.

Wenn möglich wird die erste Netzwerkkarte mit einer Verbindung, die bei der Installation verfügbar ist, automatisch zur Verwendung der automatischen Adressenkonfiguration mit DHCP konfiguriert. In SUSE Linux Enterprise Desktop mit standardmäßig aktivem NetworkManager sind alle Netzwerkkarten konfiguriert.

DHCP sollten Sie auch verwenden, wenn Sie eine DSL-Leitung verwenden, Ihr ISP (Internet Service Provider) Ihnen aber keine statische IP-Adresse zugewiesen hat. Wenn Sie DHCP verwenden möchten, konfigurieren Sie dessen Einstellungen im Dialogfeld *Netzwerkeinstellungen* des YaST-Konfigurationsmoduls für Netzwerkkarten auf dem Karteireiter *Globale Optionen* unter *Optionen für DHCP-Client*. Geben Sie unter *Broadcast-Antwort anfordern* an, ob der DHCP-Client den Server anweisen soll, seine Antworten immer per Broadcast zu versenden. Diese Einstellung ist vermutlich erfor-

derlich, wenn Sie Ihren Computer als mobilen Client in verschiedenen Netzwerken verwenden. In einer virtuellen Hostumgebung, in der mehrere Hosts über dieselbe Schnittstelle kommunizieren, müssen diese anhand der *Kennung für DHCP-Client* unterschieden werden.

DHCP eignet sich gut zur Client-Konfiguration, aber zur Server-Konfiguration ist es nicht ideal. Wenn Sie eine statische IP-Adresse festlegen möchten, gehen Sie wie folgt vor:

1 Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.

2 Wählen Sie auf dem Karteireiter *Adresse* die Option *Statisch zugewiesene IP-Adresse* aus.

3 Geben Sie die *IP-Adresse* ein. Es können beide Adressen, IPv4 und IPv6, verwendet werden. Geben Sie die Netzwerkmaske in *Teilnetzmaske* ein. Wenn die IPv6-Adresse verwendet wird, benutzen Sie *Teilnetzmaske* für die Präfixlänge im Format `/64`.

Optional kann ein voll qualifizierter *Hostname* für diese Adresse eingegeben werden, der in die Konfigurationsdatei `/etc/hosts` geschrieben wird.

4 Klicken Sie auf *Weiter*.

5 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Wenn Sie die statische Adresse verwenden, werden die Namenserver und das Standard-Gateway nicht automatisch konfiguriert. Informationen zur Konfiguration von Namenservern finden Sie unter Abschnitt 23.4.1.4, „Konfigurieren des Hostnamens und DNS“ (S. 347). Informationen zur Konfiguration eines Gateways finden Sie unter Abschnitt 23.4.1.5, „Konfigurieren des Routings“ (S. 349).

Konfigurieren von Aliassen

Ein Netzwerkgerät kann mehrere IP-Adressen haben, die Aliasse genannt werden.

ANMERKUNG: Aliasse stellen eine Kompatibilitätsfunktion dar

Die so genannten Aliasse oder Labels funktionieren nur bei IPv4. Bei IPv6 werden sie ignoriert. Bei der Verwendung von `iproute2`-Netzwerkschnittstellen können eine oder mehrere Adressen vorhanden sein.

Gehen Sie folgendermaßen vor, wenn Sie einen Alias für Ihre Netzwerkkarte mithilfe von YaST einrichten möchten:

1 Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.

2 Klicken Sie auf dem Karteireiter *Adresse* > *Zusätzliche Adressen* auf *Hinzufügen*.

3 Geben Sie den *Aliasnamen*, die *IP-Adresse* und die *Netzmaske* ein. Nehmen Sie den Schnittstellennamen nicht in den Aliasnamen auf.

4 Klicken Sie auf *OK*.

5 Klicken Sie auf *Weiter*.

6 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Ändern des Gerätenamens und der Udev-Regeln

Der Gerätename der Netzwerkkarte kann während des laufenden Betriebs geändert werden. Es kann auch festgelegt werden, ob udev die Netzwerkkarte über die Hardware-Adresse (MAC) oder die Bus-ID erkennen soll. Die zweite Option ist bei großen Servern vorzuziehen, um einen Austausch der Karten unter Spannung zu erleichtern. Mit YaST legen Sie diese Optionen wie folgt fest:

1 Wählen Sie im YaST-Modul Netzwerkeinstellungen auf dem Karteireiter *Übersicht* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.

2 Öffnen Sie den Karteireiter *Hardware*. Der aktuelle Gerätename wird unter *Udev-Regeln* angezeigt. Klicken Sie auf *Ändern*.

3 Wählen Sie aus, ob udev die Karte über die *MAC-Adresse* oder die *Bus-ID* erkennen soll. Die aktuelle MAC-Adresse und Bus-ID der Karte werden im Dialogfeld angezeigt.

4 Aktivieren Sie zum Ändern des Gerätenamens die Option *Gerätenamen ändern* und bearbeiten Sie den Namen.

5 Klicken Sie auf *OK* und *Weiter*.

6 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Ändern des Kernel-Treibers für Netzwerkkarten

Für einige Netzwerkkarten sind eventuell verschiedene Kernel-Treiber verfügbar. Wenn die Karte bereits konfiguriert ist, ermöglicht YaST die Auswahl eines zu verwendenden Kernel-Treibers in einer Liste verfügbarer Treiber. Es ist auch möglich, Optionen für den Kernel-Treiber anzugeben. Mit YaST legen Sie diese Optionen wie folgt fest:

1 Wählen Sie im YaST-Modul Netzwerkeinstellungen auf dem Karteireiter *Übersicht* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.

2 Öffnen Sie den Karteireiter *Hardware*.

3 Wählen Sie den zu verwendenden Kernel-Treiber unter *Modulname* aus. Geben Sie die entsprechenden Optionen für den ausgewählten Treiber unter *Optionen* im Format `Option=Wert` ein. Wenn mehrere Optionen verwendet werden, sollten sie durch Leerzeichen getrennt sein.

4 Klicken Sie auf *OK* und *Weiter*.

5 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Aktivieren des Netzwerkgeräts

Wenn Sie die traditionelle Methode mit ifup verwenden, können Sie Ihr Gerät so konfigurieren, dass es wahlweise beim Systemstart, bei der Verbindung per Kabel, beim Erkennen der Karte, manuell oder nie startet. Wenn Sie den Gerätestart ändern möchten, gehen Sie wie folgt vor:

1. Wählen Sie in YaST unter *Netzwerkgeräte* > *Netzwerkeinstellungen* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.

2. In der Karteireiter *Allgemein* wählen Sie den gewünschten Eintrag unter *Geräte-Aktivierung*.

   Wählen Sie *Beim Systemstart*, um das Gerät beim Booten des Systems zu starten. Wenn *Bei Kabelanschluss* aktiviert ist, wird die Schnittstelle auf physikalische Netzwerkverbindungen überwacht. Wenn *Falls hot-plugged* aktiviert ist, wird die Schnittstelle eingerichtet, sobald sie verfügbar ist. Dies gleicht der Option *Bei Systemstart*, führt jedoch nicht zu einem Fehler beim Systemstart, wenn die Schnittstelle nicht vorhanden ist. Wählen Sie *Manuell*, wenn Sie die Schnittstelle manuell mit `ifup` steuern möchten. Wählen Sie *Nie*, wenn das Gerät gar nicht gestartet werden soll. *Bei NFSroot* verhält sich ähnlich wie *Beim Systemstart*, allerdings fährt das Kommando `rcnetwork stop` die Schnittstelle bei dieser Einstellung nicht herunter. Diese Einstellung empfiehlt sich bei einem NFS- oder iSCSI-Root-Dateisystem.

3. Klicken Sie auf *Weiter*.

4. Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Normalerweise können Netzwerk-Schnittstellen nur vom Systemadministrator aktiviert und deaktiviert werden. Wenn Benutzer in der Lage sein sollen, diese Schnittstelle über KInternet zu aktivieren, wählen Sie *Gerätesteuerung für Nicht-Root-Benutzer über KInternet aktivieren* aus.

Einrichten der Größe der maximalen Transfereinheit

Sie können eine maximale Transfereinheit (MTU) für die Schnittstelle festlegen. MTU bezieht sich auf die größte zulässige Paketgröße in Byte. Eine größere MTU bringt eine höhere Bandbreiteneffizienz. Große Pakete können jedoch eine langsame Schnittstelle für einige Zeit belegen und die Verzögerung für nachfolgende Pakete vergrößern.

1. Wählen Sie in YaST unter *Netzwerkgeräte* > *Netzwerkeinstellungen* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.

2. Wählen Sie im Karteireiter *Allgemein* den gewünschten Eintrag aus der Liste *Set MTU* (MTU festlegen).

3. Klicken Sie auf *Weiter*.

4 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Konfigurieren der Firewall

Sie müssen nicht die genaue Firewall-Konfiguration durchführen, wie unter Section "Configuring the Firewall with YaST" (Chapter 15, *Masquerading and Firewalls*, ↑*Security Guide*) beschrieben. Sie können einige grundlegende Firewall-Einstellungen für Ihr Gerät als Teil der Gerätekonfiguration festlegen. Führen Sie dazu die folgenden Schritte aus:

1 Öffnen Sie das YaST-Modul *Netzwerkgeräte* > *Netzwerkeinstellungen*. Wählen Sie im Karteireiter *Übersicht* eine Karte aus der Liste erkannter Karten und klicken Sie auf *Bearbeiten*.

2 Öffnen Sie den Karteireiter *Allgemein* des Dialogfelds *Netzwerkeinstellungen*.

3 Legen Sie die Firewall-Zone fest, der Ihre Schnittstelle zugewiesen werden soll. Mit den zur Verfügung stehenden Optionen können Sie

Firewall deaktiviert
: Diese Option ist nur verfügbar, wenn die Firewall deaktiviert ist und die Firewall überhaupt nicht ausgeführt wird. Verwenden Sie diese Option nur, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird.

Automatisches Zuweisen von Zonen
: Diese Option ist nur verfügbar, wenn die Firewall aktiviert ist. Die Firewall wird ausgeführt und die Schnittstelle wird automatisch einer Firewall-Zone zugewiesen. Die Zone, die das Stichwort `Beliebig` enthält, oder die externe Zone wird für solch eine Schnittstelle verwendet.

Interne Zone (ungeschützt)
: Die Firewall wird ausgeführt, aber es gibt keine Regeln, die diese Schnittstelle schützen. Verwenden Sie diese Option, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird. Sie ist auch nützlich für die Schnittstellen, die mit dem internen Netzwerk verbunden sind,wenn der Computer über mehrere Netzwerkschnittstellen verfügt.

Demilitarisierte Zone
: Eine demilitarisierte Zone ist eine zusätzliche Verteidigungslinie zwischen einem internen Netzwerk und dem (feindlichen) Internet. Die dieser Zone zugewiesenen Hosts können vom internen Netzwerk und vom Internet erreicht werden, können jedoch nicht auf das interne Netzwerk zugreifen.

Externe Zone
: Die Firewall wird an dieser Schnittstelle ausgeführt und schützt sie vollständig vor anderem (möglicherweise feindlichem) Netzwerkverkehr. Dies ist die Standardoption.

4 Klicken Sie auf *Weiter*.

5 Aktivieren Sie die Konfiguration, indem Sie auf *OK* klicken.

23.4.1.3 Konfigurieren einer unerkannten Netzwerkkarte

Ihre Karte wird unter Umständen nicht richtig erkannt. In diesem Fall erscheint sie nicht in der Liste der erkannten Karten. Wenn Sie sich nicht sicher sind, ob Ihr System über einen Treiber für die Karte verfügt, können Sie sie manuell konfigurieren. Sie können auch spezielle Netzwerkgerätetypen konfigurieren, z. B. Bridge, Bond, TUN oder TAP. So konfigurieren Sie eine nicht erkannte Netzwerkkarte (oder ein spezielles Gerät):

1 Klicken Sie im Dialogfeld *Netzwerkgeräte* > *Netzwerkeinstellungen* > *Übersicht* in YaST auf *Hinzufügen*.

2 Legen Sie den *Gerätetyp* der Schnittstelle im Dialogfeld *Hardware* mit Hilfe der verfügbaren Optionen fest und geben Sie einen *Konfigurationsnamen* ein. Wenn es sich bei der Netzwerkkarte um ein PCMCIA- oder USB-Gerät handelt, aktivieren Sie das entsprechende Kontrollkästchen und schließen Sie das Dialogfeld durch Klicken auf *Weiter*. Ansonsten können Sie den Kernel *Modulname* definieren, der für die Karte verwendet wird, sowie gegebenenfalls dessen *Optionen*.

   Unter *Ethtool-Optionen* können Sie die von `ifup` für die Schnittstelle verwendeten `Ethtool`-Optionen einstellen. Die verfügbaren Optionen werden auf der man-Seite `ethtool` beschrieben. Wenn die Optionszeichenkette mit einem `-` beginnt (z. B. `-K` *`Schnittstellenname`* `rx on`), wird das zweite Wort der Zeichenkette

durch den aktuellen Schnittstellennamen ersetzt. Andernfalls (z. B. bei `autoneg off speed 10`) stellt `ifup` die Zeichenkette `-s` *`Schnittstellenname`* voran.

3 Klicken Sie auf *Weiter*.

4 Konfigurieren Sie die benötigten Optionen wie die IP-Adresse, die Geräteaktivierung oder die Firewall-Zone für die Schnittstelle auf den Karteireitern *Allgemein*, *Adresse* und *Hardware*. Weitere Informationen zu den Konfigurationsoptionen finden Sie in Abschnitt 23.4.1.2, „Ändern der Konfiguration einer Netzwerkkarte" (S. 340).

5 Wenn Sie für den Gerätetyp der Schnittstelle die Option *Drahtlos* gewählt haben, konfigurieren Sie im nächsten Dialogfeld die drahtlose Verbindung. Weitere Informationen zur Konfiguration drahtloser Geräte erhalten Sie unter Kapitel 20, *Wireless LAN* (S. 273).

6 Klicken Sie auf *Weiter*.

7 Klicken Sie auf *OK*, um die neue Netzwerkkonfiguration zu aktivieren.

23.4.1.4 Konfigurieren des Hostnamens und DNS

Wenn Sie die Netzwerkkonfiguration während der Installation noch nicht geändert haben und die verkabelte Karte bereits verfügbar war, wurde automatisch ein Hostname für Ihren Computer erstellt und DHCP wurde aktiviert. Dasselbe gilt für die Namensservicedaten, die Ihr Host für die Integration in eine Netzwerkumgebung benötigt. Wenn DHCP für eine Konfiguration der Netzwerkadresse verwendet wird, wird die Liste der Domain Name Server automatisch mit den entsprechenden Daten versorgt. Falls eine statische Konfiguration vorgezogen wird, legen Sie diese Werte manuell fest.

Wenn Sie den Namen Ihres Computers und die Namenserver-Suchliste ändern möchten, gehen Sie wie folgt vor:

1 Wechseln Sie zum Karteireiter *Netzwerkeinstellungen* > *Hostname/DNS* im Modul *Netzwerkgeräte* in YaST.

2 Geben Sie den *Hostnamen* und bei Bedarf auch den *Domänennamen* ein. Die Domäne ist besonders wichtig, wenn der Computer als Mailserver fungiert. Der Hostname ist global und gilt für alle eingerichteten Netzwerkschnittstellen.

Wenn Sie zum Abrufen einer IP-Adresse DHCP verwenden, wird der Hostname Ihres Computers automatisch durch DHCP festgelegt. Sie sollten dieses Verhalten deaktivieren, wenn Sie Verbindungen zu verschiedenen Netzwerken aufbauen, da Sie verschiedene Hostnamen zuweisen können und das Ändern des Hostnamens beim Ausführen den grafischen Desktop verwirren kann. Zum Deaktivieren von DHCP, damit Sie eine IP-Adresse erhalten, deaktivieren Sie *Hostnamen über DHCP ändern*.

Mithilfe von *Hostnamen zu Loopback-IP zuweisen* wird der Hostname mit der IP-Adresse `127.0.0.2` (Loopback) in `/etc/hosts` verknüpft. Diese Option ist hilfreich, wenn der Hostname jederzeit, auch ohne aktives Netzwerk, auflösbar sein soll.

3 Legen Sie unter *DNS-Konfiguration ändern* fest, wie die DNS-Konfiguration (Namenserver, Suchliste, Inhalt der Datei `/etc/resolv.conf`) geändert wird.

Wenn die Option *Standardrichtlinie verwenden* ausgewählt ist, wird die Konfiguration vom Skript `netconfig` verwaltet, das die statisch definierten Daten (mit YaST oder in den Konfigurationsdateien) mit dynamisch bezogenen Daten (vom DHCP-Client oder NetworkManager) zusammenführt. Diese Standardrichtlinie ist in den meisten Fällen ausreichend.

Wenn die Option *Nur manuell* ausgewählt ist, darf `netconfig` die Datei `/etc/resolv.conf` nicht ändern. Jedoch kann diese Datei manuell bearbeitet werden.

Wenn die Option *Benutzerdefinierte Richtlinie* ausgewählt ist, muss eine Zeichenkette für die *benutzerdefinierte Richtlinienregel* angegeben werden, welche die Zusammenführungsrichtlinie definiert. Die Zeichenkette besteht aus einer durch Kommas getrennten Liste mit Schnittstellennamen, die als gültige Quelle für Einstellungen betrachtet werden. Mit Ausnahme vollständiger Schnittstellennamen sind auch grundlegende Platzhalter zulässig, die mit mehreren Schnittstellen übereinstimmen. Beispiel: `eth* ppp?` richtet sich zuerst an alle eth- und dann an alle ppp0-ppp9-Schnittstellen. Es gibt zwei spezielle Richtlinienwerte, die angeben, wie die statischen Einstellungen angewendet werden, die in der Datei `/etc/sysconfig/network/config` definiert sind:

`STATIC`
: Die statischen Einstellungen müssen mit den dynamischen Einstellungen zusammengeführt werden.

`STATIC_FALLBACK`
: Die statischen Einstellungen werden nur verwendet, wenn keine dynamische Konfiguration verfügbar ist.

Weitere Informationen finden Sie unter `man 8 netconfig`.

4. Geben Sie die *Namenserver* ein und füllen Sie die *Domänensuchliste* aus. Nameserver müssen in der IP-Adresse angegeben werden (z. B. 192.168.1.116), nicht im Hostnamen. Namen, die im Karteireiter *Domänensuche* angegeben werden, sind Namen zum Auflösen von Hostnamen ohne angegebene Domäne. Wenn mehr als eine *Suchdomäne* verwendet wird, müssen die Domänen durch Kommas oder Leerzeichen getrennt werden.

5. Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Der Hostname kann auch mit YaST über die Kommandozeile bearbeitet werden. Die Änderungen in YaST treten sofort in Kraft (im Gegensatz zur manuellen Bearbeitung der Datei `/etc/HOSTNAME`). Zum Ändern des Hostnamens führen Sie das folgende Kommando aus:

```
yast dns edit hostname=hostname
```

Zum Ändern der Namenserver führen Sie die folgenden Kommandos aus:

```
yast dns edit nameserver1=192.168.1.116
yast dns edit nameserver2=192.168.1.116
yast dns edit nameserver3=192.168.1.116
```

23.4.1.5 Konfigurieren des Routings

Damit Ihre Maschine mit anderen Maschinen und Netzwerken kommuniziert, müssen Routing-Daten festgelegt werden. Dann nimmt der Netzwerkverkehr den korrekten Weg. Wird DHCP verwendet, werden diese Daten automatisch angegeben. Wird eine statische Konfiguration verwendet, müssen Sie die Daten manuell angeben.

1. Navigieren Sie in YaST zu *Netzwerkeinstellungen* > *Routing*.

2. Geben Sie die IP-Adresse für das *Standard-Gateway* ein (gegebenenfalls IPv4 und IPv6). Der Standard-Gateway entspricht jedem möglichen Ziel, wenn aber ein anderer Eintrag der erforderlichen Adresse entspricht, wird diese anstelle der Standardroute verwendet.

3. In der *Routing-Tabelle* können weitere Einträge vorgenommen werden. Geben Sie die IP-Adresse für das *Ziel*-Netzwerk, die IP-Adresse des *Gateways* und die *Netzmaske* ein. Wählen Sie das *Gerät* aus, durch das der Datenverkehr zum definierten Netzwerk geroutet wird (das Minuszeichen steht für ein beliebiges Gerät). Verwenden Sie das Minuszeichen `-`, um diese Werte frei zu lassen. Verwenden Sie `default` im Feld *Ziel*, um in der Tabelle ein Standard-Gateway einzugeben.

   ANMERKUNG

   Wenn mehrere Standardrouten verwendet werden, kann die Metrik-Option verwendet werden, um festzulegen, welche Route eine höhere Priorität hat. Geben Sie zur Angabe der Metrik-Option `- Metrik` *`Nummer`* unter *Optionen* ein. Die Route mit der höchsten Metrik wird als Standard verwendet. Wenn das Netzwerkgerät getrennt wird, wird seine Route entfernt und die nächste verwendet. Der aktuelle Kernel verwendet jedoch keine Metrik bei statischem Routing, sondern nur ein Routing-Dämon wie multipathd.

4. Wenn das System ein Router ist, aktivieren Sie die Option *IP-Weiterleitung* in den *Netzwerkeinstellungen*.

5. Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

23.4.2 Modem

Im YaST-Kontrollzentrum greifen Sie mit *Netzwerkgeräte* > *Modem* auf die Modem-Konfiguration zu. Wenn Ihr Modem nicht automatisch erkannt wurde, wechseln Sie zum Karteireiter *Modemgeräte* und öffnen Sie das Dialogfeld für manuelle Konfiguration, indem Sie auf *Hinzufügen* klicken. Geben Sie unter *Modemgerät* die Schnittstelle an, an die das Modem angeschlossen ist.

TIPP: CDMA- und GPRS-Modems

Konfigurieren Sie unterstützte CDMA- und GPRS-Modems mit dem YaST-*Modem*-Modul wie reguläre Modems.

Abbildung 23.4 *Modemkonfiguration*



Wenn eine Telefonanlage zwischengeschaltet ist, müssen Sie ggf. eine Vorwahl für die Amtsholung eingeben. Dies ist in der Regel die Null. Sie können diese aber auch in der Bedienungsanleitung der Telefonanlage finden. Zudem können Sie festlegen, ob Ton- oder Impulswahl verwendet, der Lautsprecher eingeschaltet und der Wählton abgewartet werden soll. Letztere Option sollte nicht verwendet werden, wenn Ihr Modem an einer Telefonanlage angeschlossen ist.

Legen Sie unter *Details* die Baudrate und die Zeichenketten zur Modeminitialisierung fest. Ändern Sie die vorhandenen Einstellungen nur, wenn das Modem nicht automatisch erkannt wird oder es spezielle Einstellungen für die Datenübertragung benötigt. Dies ist vor allem bei ISDN-Terminaladaptern der Fall. Schließen Sie das Dialogfeld mit *OK*. Wenn Sie die Kontrolle des Modems an normale Benutzer ohne Root-Berechtigung abgeben möchten, aktivieren Sie *Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen*. Auf diese Weise kann ein Benutzer ohne Administratorberechtigungen eine Schnittstelle aktivieren oder deaktivieren. Geben Sie unter *Regulärer Ausdruck für Vorwahl zur Amtsholung* einen regulären Ausdruck an. Dieser muss der vom Benutzer unter *Dial Prefix* (Vorwahl) in KInternet bearbeitbaren Vorwahl entsprechen. Wenn dieses Feld leer ist, kann ein Benutzer ohne Administratorberechtigungen keine andere *Vorwahl* festlegen.

Wählen Sie im nächsten Dialogfeld den ISP (Internet Service Provider). Wenn Sie Ihren Provider aus einer Liste der für Ihr Land verfügbaren Provider auswählen möchten, aktivieren Sie *Land*. Sie können auch auf *Neu* klicken, um ein Dialogfeld zu öffnen, in dem Sie die Daten Ihres ISPs eingeben können. Dazu gehören ein Name für die Einwahlverbindung und den ISP sowie die vom ISP zur Verfügung gestellten Benutzer- und Kennwortdaten für die Anmeldung. Aktivieren Sie *Immer Passwort abfragen*, damit immer eine Passwortabfrage erfolgt, wenn Sie eine Verbindung herstellen.

Im letzten Dialogfeld können Sie zusätzliche Verbindungsoptionen angeben:

Dial-On-Demand
: Wenn Sie *Dial-on-Demand* aktivieren, müssen Sie mindestens einen Namenserver angeben. Verwenden Sie diese Funktion nur, wenn Sie über eine günstige Internet-Verbindung oder eine Flatrate verfügen, da manche Programme in regelmäßigen Abständen Daten aus dem Internet abfragen.

Während Verbindung DNS ändern
: Diese Option ist standardmäßig aktiviert, d. h. die Adresse des Namenservers wird bei jeder Verbindung mit dem Internet automatisch aktualisiert.

DNS automatisch abrufen
: Wenn der Provider nach dem Herstellen der Verbindung seinen DNS-Server nicht überträgt, deaktivieren Sie diese Option und geben Sie die DNS-Daten manuell ein.

Automatische Verbindungswiederherstellung
: Wenn aktiviert, wird nach einem Fehler automatisch versucht, die Verbindung wiederherzustellen.

Ignoriere Eingabeaufforderung
: Diese Option deaktiviert die Erkennung der Eingabeaufforderungen des Einwahlservers. Aktivieren Sie diese Option, wenn der Verbindungsaufbau sehr lange dauert oder die Verbindung nicht zustande kommt.

Externe Firewall-Schnittstelle
: Durch Auswahl dieser Option wird die Firewall aktiviert und die Schnittstelle als extern festgelegt. So sind Sie für die Dauer Ihrer Internetverbindung vor Angriffen von außen geschützt.

Idle-Time-Out (Sekunden)
Mit dieser Option legen Sie fest, nach welchem Zeitraum der Netzwerkinaktivität die Modemverbindung automatisch getrennt wird.

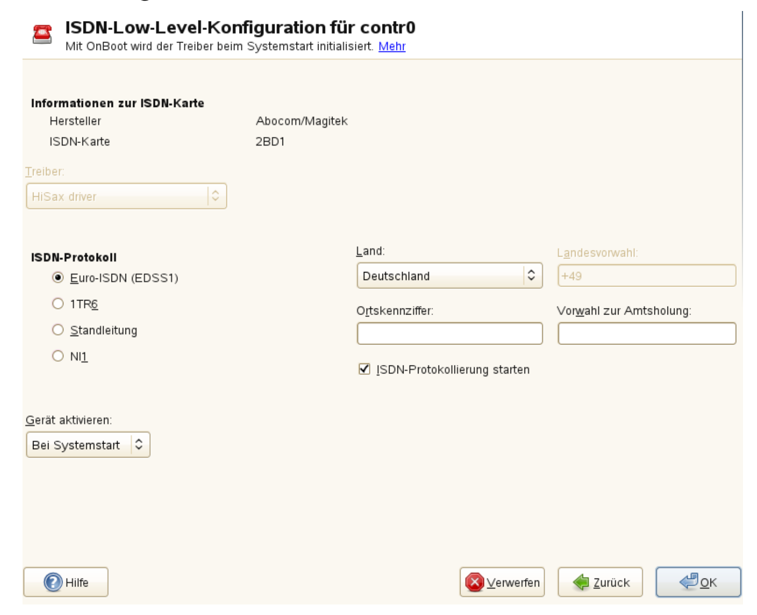
IP-Details
Diese Option öffnet das Dialogfeld für die Adresskonfiguration. Wenn Ihr ISP Ihrem Host keine dynamische IP-Adresse zuweist, deaktivieren Sie die Option *Dynamische IP-Adresse* und geben Sie die lokale IP-Adresse des Hosts und anschließend die entfernte IP-Adresse ein. Diese Informationen erhalten Sie von Ihrem ISP. Lassen Sie die Option *Standard-Route* aktiviert und schließen Sie das Dialogfeld mit *OK*.

Durch Auswahl von *Weiter* gelangen Sie zum ursprünglichen Dialogfeld zurück, in dem eine Zusammenfassung der Modemkonfiguration angezeigt wird. Schließen Sie das Dialogfeld mit *OK*.

23.4.3 ISDN

Dieses Modul ermöglicht die Konfiguration einer oder mehrerer ISDN-Karten in Ihrem System. Wenn YaST Ihre ISDN-Karte nicht erkannt hat, klicken Sie auf dem Karteireiter *ISDN-Geräte* auf *Hinzufügen* und wählen Sie Ihre Karte manuell aus. Theoretisch können Sie mehrere Schnittstellen einrichten, im Normalfall ist dies aber nicht notwendig, da Sie für eine Schnittstelle mehrere Provider einrichten können. Die nachfolgenden Dialogfelder dienen dann dem Festlegen der verschiedenen ISDN-Optionen für den ordnungsgemäßen Betrieb der Karte.

Abbildung 23.5 *ISDN-Konfiguration*



Wählen Sie im nächsten Dialogfeld, das in Abbildung 23.5, „ISDN-Konfiguration" (S. 354) dargestellt ist, das zu verwendende Protokoll. Der Standard ist *Euro-ISDN (EDSS1)*, aber für ältere oder größere Telefonanlagen wählen Sie *1TR6*. Für die USA gilt *NI1*. Wählen Sie das Land in dem dafür vorgesehenen Feld aus. Die entsprechende Landeskennung wird im Feld daneben angezeigt. Geben Sie dann noch die *Ortsnetzkennzahl* und ggf. die *Vorwahl zur Amtsholung* ein. Wenn nicht der gesamte ISDN-Datenverkehr protokolliert werden soll, deaktivieren Sie die Option *ISDN-Protokollierung starten*.

Geräte-Aktivierung definiert, wie die ISDN-Schnittstelle gestartet werden soll: *Beim Systemstart* initialisiert den ISDN-Treiber bei jedem Systemstart. *Manuell* erfordert, dass Sie den ISDN-Treiber als `root` mit dem Befehl `rcisdn start` laden. *Falls hot-plugged* wird für PCMCIA- oder USB-Geräte verwendet. Diese Option lädt den Treiber, nachdem das Gerät eingesteckt wurde. Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *OK*.

Im nächsten Dialogfeld können Sie den Schnittstellentyp für die ISDN-Karte angeben und weitere ISPs zu einer vorhandenen Schnittstelle hinzufügen. Schnittstellen können in den Betriebsarten `SyncPPP` oder `RawIP` angelegt werden. Die meisten ISPs verwenden jedoch den `SyncPPP`-Modus, der im Folgenden beschrieben wird.

Abbildung 23.6 *Konfiguration der ISDN-Schnittstelle*



Die Nummer, die Sie unter *Eigene Telefonnummer* eingeben, ist vom jeweiligen Anschlussszenario abhängig:

ISDN-Karte direkt an der Telefondose
: Eine standardmäßige ISDN-Leitung bietet Ihnen drei Rufnummern (so genannte MSNs, Multiple Subscriber Numbers). Auf Wunsch können (auch) bis zu zehn Rufnummern zur Verfügung gestellt werden. Eine dieser MSNs muss hier eingegeben werden, allerdings ohne Ortsnetzkennzahl. Sollten Sie eine falsche Nummer eintragen, wird Ihr Netzbetreiber die erste Ihrem ISDN-Anschluss zugeordnete MSN verwenden.

ISDN-Karte an einer Telefonanlage
: Auch hier kann die Konfiguration je nach installierten Komponenten variieren:

1. Kleinere Telefonanlagen für den Hausgebrauch verwenden für interne Anrufe in der Regel das Euro-ISDN-Protokoll (EDSS1). Diese Telefonanlagen haben einen internen S0-Bus und verwenden für die angeschlossenen Geräte interne Rufnummern.

   Für die Angabe der MSN verwenden Sie eine der internen Rufnummern. Eine der möglichen MSNs Ihrer Telefonanlage sollte funktionieren, sofern für diese der Zugriff nach außen freigeschaltet ist. Im Notfall funktioniert eventuell auch eine einzelne Null. Weitere Informationen dazu entnehmen Sie bitte der Dokumentation Ihrer Telefonanlage.

2. Größere Telefonanlagen (z. B. in Unternehmen) verwenden für die internen Anschlüsse das Protokoll 1TR6. Die MSN heißt hier EAZ und ist üblicherweise die Durchwahl. Für die Konfiguration unter Linux ist die Eingabe der letzten drei Stellen der EAZ in der Regel ausreichend. Im Notfall probieren Sie die Ziffern 1 bis 9.

Wenn die Verbindung vor der nächsten zu zahlenden Gebühreneinheit getrennt werden soll, aktivieren Sie *ChargeHUP*. Dies funktioniert unter Umständen jedoch nicht mit jedem ISP. Durch Auswahl der entsprechenden Option können Sie auch die Kanalbündelung (Multilink-PPP) aktivieren. Sie können die Firewall für die Verbindung aktivieren, indem Sie *Externe Firewall-Schnittstelle* und *Firewall neu starten* auswählen. Wenn Sie normalen Benutzern ohne Administratorberechtigung die Aktivierung und Deaktivierung der Schnittstelle erlauben möchten, aktivieren Sie *Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen*.

Details öffnet ein Dialogfeld, das für die Implementierung komplexerer Verbindungsszenarien ausgelegt und aus diesem Grund für normale Heimbenutzer nicht relevant ist. Schließen Sie das Dialogfeld *Details* mit *OK*.

Im nächsten Dialogfeld konfigurieren Sie die Einstellungen der IP-Adressen. Wenn Ihr Provider Ihnen keine statische IP-Adresse zugewiesen hat, wählen Sie *Dynamische IP-Adresse*. Anderenfalls tragen Sie gemäß den Angaben Ihres Providers die lokale IP-Adresse Ihres Rechners sowie die entfernte IP-Adresse in die dafür vorgesehenen Felder ein. Soll die anzulegende Schnittstelle als Standard-Route ins Internet dienen, aktivieren Sie *Standard-Route*. Beachten Sie, dass jeweils nur eine Schnittstelle pro System als Standard-Route in Frage kommt. Schließen Sie das Dialogfeld mit *Weiter*.

Im folgenden Dialogfeld können Sie Ihr Land angeben und einen ISP wählen. Bei den in der Liste aufgeführten ISPs handelt es sich um Call-By-Call-Provider. Wenn Ihr ISP in der Liste nicht aufgeführt ist, wählen Sie *Neu*. Dadurch wird das Dialogfeld *Provider-Parameter* geöffnet, in dem Sie alle Details zu Ihrem ISP eingeben können. Die Telefonnummer darf keine Leerzeichen oder Kommas enthalten. Geben Sie dann den Benutzernamen und das Passwort ein, den bzw. das Sie von Ihrem ISP erhalten haben. Wählen Sie anschließend *Weiter*.

Um auf einem eigenständigen Arbeitsplatzrechner *Dial-On-Demand* verwenden zu können, müssen Sie auch den Namenserver (DNS-Server) angeben. Die meisten Provider unterstützen heute die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namenservers übergeben. Bei einem Einzelplatz-Arbeitsplatzrechner müssen Sie dennoch eine Platzhalteradresse wie `192.168.22.99` angeben. Wenn

Ihr ISP keine dynamischen DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namenserver des ISPs ein. Ferner können Sie festlegen, nach wie vielen Sekunden die Verbindung automatisch getrennt werden soll, falls in der Zwischenzeit kein Datenaustausch stattgefunden hat. Bestätigen Sie die Einstellungen mit *Weiter*. YaST zeigt eine Zusammenfassung der konfigurierten Schnittstellen an. Klicken Sie zur Aktivierung dieser Einstellungen auf *OK*.

23.4.4 Kabelmodem

In einigen Ländern wird der Zugriff auf das Internet über Kabel-TV mehr und mehr üblich. Der TV-Kabel-Abonnent erhält in der Regel ein Modem, das auf der einen Seite an die TV-Kabelbuchse und auf der anderen Seite (mit einem 10Base-TG Twisted-Pair-Kabel) an die Netzwerkkarte des Computers angeschlossen wird. Das Kabelmodem stellt dann eine dedizierte Internetverbindung mit einer statischen IP-Adresse zur Verfügung.

Richten Sie sich bei der Konfiguration der Netzwerkkarte nach den Anleitungen Ihres ISP (Internet Service Provider) und wählen Sie entweder *Dynamische Adresse* oder *Statisch zugewiesene IP-Adresse* aus. Die meisten Provider verwenden heute DHCP. Eine statische IP-Adresse ist oft Teil eines speziellen Firmenkontos.

23.4.5 DSL

Wählen Sie zum Konfigurieren des DSL-Geräts das YaST-Modul *DSL* unter *Netzwerkgeräte* aus. Dieses YaST-Modul besteht aus mehreren Dialogfeldern, in denen Sie die Parameter des DSL-Zugangs basierend auf den folgenden Protokollen festlegen können:

- PPP über Ethernet (PPPoE)
- PPP über ATM (PPPoATM)
- CAPI für ADSL (Fritz-Karten)
- Tunnel-Protokoll für Point-to-Point (PPTP) - Österreich

Im Dialogfeld *Überblick über die DSL-Konfiguration* finden Sie auf dem Karteireiter *DSL-Geräte* eine Liste der installierten DSL-Geräte. Zur Änderung der Konfiguration eines DSL-Geräts wählen Sie das Gerät in der Liste aus und klicken Sie auf *Bearbeiten*.

Wenn Sie ein neues DSL-Gerät manuell konfigurieren möchten, klicken Sie auf *Hinzufügen*.

Zur Konfiguration eines DSL-Zugangs auf der Basis von PPPoE oder PPTP ist es erforderlich, die entsprechende Netzwerkkarte korrekt zu konfigurieren. Falls noch nicht geschehen, konfigurieren Sie zunächst die Karte, indem Sie *Netzwerkkarten konfigurieren* auswählen (siehe Abschnitt 23.4.1, „Konfigurieren der Netzwerkkarte mit YaST“ (S. 337)). Bei DSL-Verbindungen können die Adressen zwar automatisch vergeben werden, jedoch nicht über DHCP. Aus diesem Grund dürfen Sie die Option *Dynamic Address* (Dynamische Adresse) nicht aktivieren. Geben Sie stattdessen eine statische Dummy-Adresse für die Schnittstelle ein, z. B. `192.168.22.1`. Geben Sie unter *Subnetzmaske* `255.255.255.0` ein. Wenn Sie eine Einzelplatz-Arbeitsstation konfigurieren, lassen Sie das Feld *Standard-Gateway* leer.

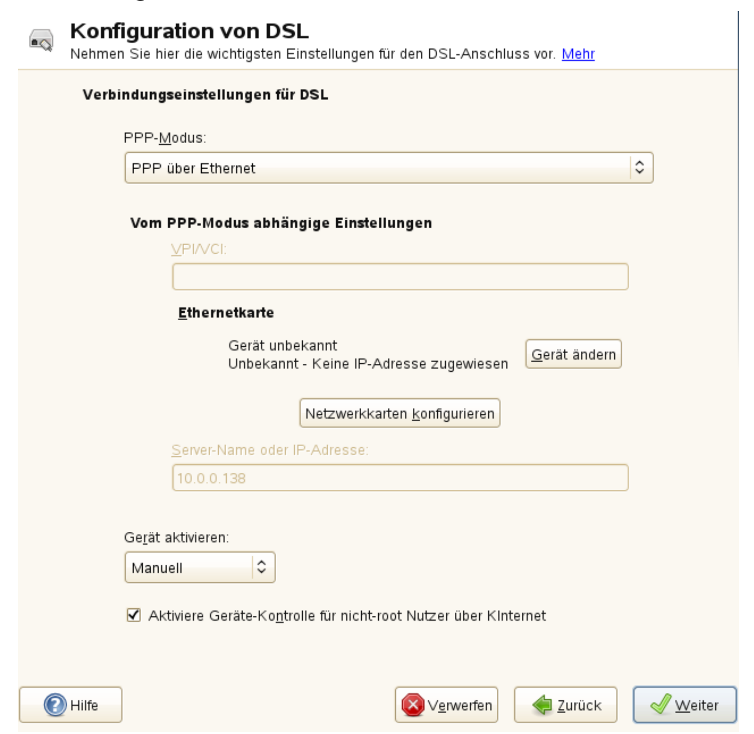
TIPP

Die Werte in den Feldern *IP-Adresse* und *Subnetzmaske* sind lediglich Platzhalter. Sie haben für den Verbindungsaufbau mit DSL keine Bedeutung und werden nur zur Initialisierung der Netzwerkkarte benötigt.

Wählen Sie im ersten Dialogfeld für die DSL-Konfiguration (siehe Abbildung 23.7, „DSL-Konfiguration“ (S. 359)) den *PPP-Modus* und die *Ethernetkarte*, mit der das DSL-Modem verbunden ist (in den meisten Fällen ist dies `eth0`). Geben Sie anschließend unter *Geräte-Aktivierung* an, ob die DSL-Verbindung schon beim Booten des Systems gestartet werden soll. Aktivieren Sie *Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen*, wenn Sie normalen Benutzern ohne Root-Berechtigung die Aktivierung und Deaktivierung der Schnittstelle via KInternet erlauben möchten.

Wählen Sie im nächsten Dialogfeld Ihr Land aus und treffen Sie eine Auswahl aus den ISPs, die in Ihrem Land verfügbar sind. Die Inhalte der danach folgenden Dialogfelder der DSL-Konfiguration hängen stark von den bis jetzt festgelegten Optionen ab und werden in den folgenden Abschnitten daher nur kurz angesprochen. Weitere Informationen zu den verfügbaren Optionen erhalten Sie in der ausführlichen Hilfe in den einzelnen Dialogfeldern.

Abbildung 23.7 DSL-Konfiguration



Um auf einem Einzelplatz-Arbeitsplatzrechner *Dial-On-Demand* verwenden zu können, müssen Sie auf jeden Fall den Namenserver (DNS-Server) angeben. Die meisten Provider unterstützen heute die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namenservers übergeben. Bei einem Einzelplatz-Arbeitsplatzrechner müssen Sie jedoch eine Platzhalteradresse wie `192.168.22.99` angeben. Wenn Ihr ISP keine dynamische DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namenserver des ISPs ein.

Idle-Timeout (Sekunden) definiert, nach welchem Zeitraum der Netzwerkinaktivität die Verbindung automatisch getrennt wird. Hier sind Werte zwischen 60 und 300 Sekunden empfehlenswert. Wenn *Dial-On-Demand* deaktiviert ist, kann es hilfreich sein, das Zeitlimit auf Null zu setzen, um das automatische Trennen der Verbindung zu vermeiden.

Die Konfiguration von T-DSL entspricht weitgehend der Konfiguration von DSL. Durch Auswahl von *T-Online* als Provider gelangen Sie in das YaST-Konfigurationsdialogfeld für T-DSL. In diesem Dialogfeld geben Sie einige zusätzliche Informationen

ein, die für T-DSL erforderlich sind: die Anschlusskennung, die T-Online-Nummer, die Benutzerkennung und Ihr Passwort. Diese Informationen finden Sie in den T-DSL-Anmeldeunterlagen.

23.5 NetworkManager

NetworkManager ist die ideale Lösung für Notebooks und andere portable Computer. Wenn Sie viel unterwegs sind und den NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen Netzwerken zu verschwenden.

23.5.1 NetworkManager und ifup

NetworkManager ist jedoch nicht in jedem Fall eine passende Lösung, daher können Sie immer noch zwischen der herkömmlichen Methode zur Verwaltung von Netzwerkverbindungen (ifup) und NetworkManager wählen. Wenn Ihre Netzwerkverbindung mit NetworkManager verwaltet werden soll, aktivieren Sie NetworkManager im Netzwerkeinstellungsmodul von YaST wie in Abschnitt 26.2, „Aktivieren oder Deaktivieren von NetworkManager“ (S. 400) beschrieben, und konfigurieren Sie Ihre Netzwerkverbindungen mit NetworkManager. Eine Liste der Anwendungsfälle sowie eine detaillierte Beschreibung zur Konfiguration und Verwendung von NetworkManager finden Sie in Kapitel 26, *Verwendung von NetworkManager* (S. 399).

Einige Unterschiede zwischen ifup und NetworkManager sind:

`root`-Berechtigungen

: Wenn Sie den NetworkManager für die Netzwerkeinrichtung verwenden, können Sie mithilfe eines Applets von Ihrer Desktop-Umgebung aus Ihre Netzwerkverbindung jederzeit auf einfache Weise wechseln, stoppen oder starten. Der NetworkManager ermöglicht zudem die Änderung und Konfiguration drahtloser Kartenverbindungen ohne `root`-Berechtigungen. Aus diesem Grund ist der NetworkManager die ideale Lösung für eine mobile Arbeitsstation.

: Die herkömmliche Konfiguration mit ifup bietet auch einige Methoden zum Wechseln, Stoppen oder Starten der Verbindung mit oder ohne Eingreifen des Benutzers, wie zum Beispiel benutzerverwaltete Geräte. Dazu sind jedoch immer `root`-Berechtigungen erforderlich, um ein Netzwerkgerät ändern oder konfigurieren

zu können. Dies stellt häufig ein Problem bei der mobilen Computernutzung dar, bei der es nicht möglich ist, alle Verbindungsmöglichkeiten vorzukonfigurieren.

Typen von Netzwerkverbindungen
: Sowohl die herkömmliche Konfiguration als auch der NetworkManager ermöglichen Netzwerkverbindungen mit einem drahtlosen Netzwerk (mit WEP-, WPA-PSK- und WPA-Enterprise-Zugriff) und verkabelten Netzwerken mithilfe von DHCP oder der statischen Konfiguration. Diese unterstützen auch eine Verbindung über Einwahl, DSL und VPN. Mit NetworkManager können Sie auch ein Modem für mobiles Breitband (3G) anschließen, was mit der herkömmlichen Konfiguration nicht möglich ist.

  Der NetworkManager versucht, Ihren Computer fortlaufend mit der besten verfügbaren Verbindung im Netzwerk zu halten. Wurde das Netzwerkkabel versehentlich ausgesteckt, wird erneut versucht, eine Verbindung herzustellen. Der NetworkManager sucht in der Liste Ihrer drahtlosen Verbindungen nach dem Netzwerk mit dem stärksten Signal und stellt automatisch eine Verbindung her. Wenn Sie dieselbe Funktionalität mit ifup erhalten möchten, ist einiger Konfigurationsaufwand erforderlich.

23.5.2 NetworkManager-Funktionalität und Konfigurationsdateien

Die mit NetworkManager erstellten individuellen Einstellungen für Netzwerkverbindungen werden in Konfigurationsprofilen gespeichert. Die mit NetworkManager oder YaST konfigurierten *system*-Verbindungen werden in `/etc/networkmanager/system-connections/*` oder in `/etc/sysconfig/network/ifcfg-*` gespeichert. Benutzerdefinierte Verbindungen werden in GConf für GNOME bzw. unter `$HOME/.kde4/share/apps/networkmanagement/*` für KDE gespeichert.

Falls kein Profil konfiguriert wurde, erstellt NetworkManager es automatisch und benennt es mit `Auto $INTERFACE-NAME`. Damit versucht man, in möglichst vielen Fällen (auf sichere Weise) ohne Konfiguration zu arbeiten. Falls die automatisch erstellten Profile nicht Ihren Anforderungen entsprechen, verwenden Sie die von KDE oder GNOME zur Verfügung gestellten Dialogfelder zur Konfiguration der Netzwerkverbindung, um die Profile wunschgemäß zu bearbeiten. Weitere Informationen hierzu finden Sie in Abschnitt 26.3, „Konfigurieren von Netzwerkverbindungen“ (S. 401).

23.5.3 Steuern und Sperren von NetworkManager-Funktionen

Auf zentral verwalteten Computern können bestimmte NetworkManager-Funktionen mit PolicyKit gesteuert oder deaktiviert werden, zum Beispiel, wenn ein Benutzer administratordefinierte Verbindungen bearbeiten oder ein Benutzer eigene Netzwerkkonfigurationen definieren darf. Starten Sie zum Anzeigen oder Ändern der entsprechenden NetworkManager-Richtlinien das grafische Werkzeug *Zugriffsberechtigungen* für PolicyKit. Im Baum auf der linken Seite finden Sie diese unterhalb des Eintrags *network-manager-settings*. Eine Einführung zu PolicyKit und detaillierte Informationen zur Verwendung finden Sie unter Chapter 9, *PolicyKit* (↑*Security Guide*).

23.6 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte immer die letzte Alternative sein. Wir empfehlen, YaST zu benutzen. Die folgenden Hintergrundinformationen zur Netzwerkkonfiguration können Ihnen jedoch auch bei der Arbeit mit YaST behilflich sein.

Wenn der Kernel eine Netzwerkkarte erkennt und eine entsprechende Netzwerkschnittstelle erstellt, weist er dem Gerät einen Namen zu. Dieser richtet sich nach der Reihenfolge der Geräteerkennung bzw. nach der Reihenfolge, in der die Kernel-Module geladen werden. Die vom Kernel vergebenen Standardgerätenamen lassen sich nur in sehr einfachen oder überaus kontrollierten Hardwareumgebungen vorhersagen. Auf Systemen, auf denen es möglich ist, Hardware während der Laufzeit hinzuzufügen oder zu entfernen, oder die die automatische Konfiguration von Geräten zulassen, können vom Kernel über mehrere Neustarts hinaus keine stabilen Netzwerkgerätenamen erwartet werden.

Für die Systemkonfigurationstools sind jedoch dauerhafte (persistente) Schnittstellennamen erforderlich. Dieses Problem wird durch udev gelöst. Der udev-persistente Netzgenerator (`/lib/udev/rules.d/75-persistent-net-generator.rules`) generiert eine Regel zum Hardwareabgleich (standardmäßig mit seiner Hardwareadresse) und weist eine dauerhaft eindeutige Schnittstelle für die Hardware zu. Die udev-Datenbank mit den Netzwerkschnittstellen wird in der Datei `/etc/udev/rules.d/70-persistent-net.rules` gespeichert. Pro Zeile dieser Datei wird eine Netzwerkschnittstelle beschrieben und deren persistenter Name angegeben. Die

zugewiesenen Namen können vom Systemadministrator im Eintrag `NAME=`„“ geändert werden. Die persistenten Regeln können auch mithilfe von YaST geändert werden.

Tabelle 23.5, „Skripten für die manuelle Netzwerkkonfiguration“ (S. 363) zeigt die wichtigsten an der Netzwerkkonfiguration beteiligten Skripten.

***Tabelle 23.5** Skripten für die manuelle Netzwerkkonfiguration*

Befehl	Funktion
`ifup, ifdown, ifstatus`	Die `if`-Skripten starten oder stoppen Netzwerkschnittstellen oder geben den Status der angegebenen Schnittstelle zurück. Weitere Informationen finden Sie auf der man-Seite `ifup`.
`rcnetwork`	Mit dem Skript `rcnetwork` können alle Netzwerkschnittstellen (oder nur eine bestimmte Netzwerkschnittstelle) gestartet, gestoppt oder neu gestartet werden. Verwenden Sie `rcnetwork stop` zum Anhalten, `rcnetwork start` zum Starten und `rcnetwork restart` zum Neustart von Netzwerkschnittstellen. Wenn Sie nur eine Netzwerkschnittstelle stoppen, starten oder neu starten möchten, geben Sie nach dem jeweiligen Kommando den Namen der Schnittstelle ein, zum Beispiel `rcnetwork restart eth0`. Das Kommando `rcnetwork status` zeigt den Status und die IP-Adressen der Netzwerkschnittstellen an. Außerdem gibt das Kommando an, ob auf den Schnittstellen ein DHCP-Client ausgeführt wird. Mit `rcnetwork stop-all-dhcp-clients` und `rcnetwork`

Befehl	Funktion
	`restart-all-dhcp-clients` können Sie die auf den Netzwerkschnittstellen ausgeführten DHCP-Clients stoppen und wieder starten.

Weitere Informationen zu udex und dauerhaften Gerätenamen finden Sie unter Kapitel 16, *Gerätemanagement über dynamischen Kernel mithilfe von* `udev` (S. 225).

23.6.1 Konfigurationsdateien

Dieser Abschnitt bietet einen Überblick über die Netzwerkkonfigurationsdateien und erklärt ihren Zweck sowie das verwendete Format.

23.6.1.1 /etc/sysconfig/network/ifcfg-*

Diese Dateien enthalten die Konfigurationsdaten für Netzwerkschnittstellen. Sie enthalten Informationen wie den Startmodus und die IP-Adresse. Mögliche Parameter sind auf der man-Seite für den Befehl `ifup` beschrieben. Wenn eine allgemeine Einstellung nur für eine bestimmte Bedienoberfläche verwendet werden soll, können außerdem alle Variablen aus der Datei `dhcp` in den `ifcfg-*`-Dateien verwendet werden. Jedoch sind die meisten `/etc/sysconfig/network/config`-Variablen global und lassen sich in ifcfg-Dateien nicht überschreiben. Beispielsweise sind die Variablen `NETWORKMANAGER` oder `NETCONFIG_*` global.

Informationen zu `ifcfg.template` finden Sie unter Abschnitt 23.6.1.2, „`/etc/sysconfig/network/config` und `/etc/sysconfig/network/dhcp`“ (S. 364).

23.6.1.2 /etc/sysconfig/network/config und /etc/sysconfig/network/dhcp

Die Datei `config` enthält allgemeine Einstellungen für das Verhalten von `ifup`, `ifdown` und `ifstatus`. `dhcp` enthält Einstellungen für DHCP. Die Variablen in

beiden Konfigurationsdateien sind kommentiert. Einige der Variablen von /etc/sysconfig/network/config können auch in ifcfg-*-Dateien verwendet werden, wo sie eine höherer Priorität erhalten. Die Datei /etc/sysconfig/network/ifcfg.template listet Variablen auf, die mit einer Reichweite pro Schnittstelle angegeben werden können. Jedoch sind die meisten /etc/sysconfig/network/config-Variablen global und lassen sich in ifcfg-Dateien nicht überschreiben. Beispielsweise sind die Variablen NETWORKMANAGER oder NETCONFIG_* global.

23.6.1.3 /etc/sysconfig/network/routes und /etc/sysconfig/network/ifroute-*

Hier wird das statische Routing von TCP/IP-Paketen festgelegt. Alle statischen Routen, die für verschiedenen Systemaufgaben benötigt werden, können in die Datei /etc/sysconfig/network/routes eingegeben werden: Routen zu einem Host, Routen zu einem Host über Gateways und Routen zu einem Netzwerk. Definieren Sie für jede Schnittstelle, die individuelles Routing benötigt, eine zusätzliche Konfigurationsdatei: /etc/sysconfig/network/ifroute-*. Ersetzen Sie * durch den Namen der Schnittstelle. Die folgenden Einträge werden in die Routing-Konfigurationsdatei aufgenommen:

```
# Destination     Dummy/Gateway     Netmask            Device
#
127.0.0.0         0.0.0.0           255.255.255.0      lo
204.127.235.0     0.0.0.0           255.255.255.0      eth0
default           204.127.235.41    0.0.0.0            eth0
207.68.156.51     207.68.145.45     255.255.255.255    eth1
192.168.0.0       207.68.156.51     255.255.0.0        eth1
```

Das Routenziel steht in der ersten Spalte. Diese Spalte kann die IP-Adresse eines Netzwerks oder Hosts bzw., im Fall von *erreichbaren* Namenservern, den voll qualifizierten Netzwerk- oder Hostnamen enthalten.

Die zweite Spalte enthält das Standard-Gateway oder ein Gateway, über das der Zugriff auf einen Host oder ein Netzwerk erfolgt. Die dritte Spalte enthält die Netzmaske für Netzwerke oder Hosts hinter einem Gateway. Die Maske 255.255.255.255 gilt beispielsweise für einen Host hinter einem Gateway.

Die vierte Spalte ist nur für Netzwerke relevant, die mit dem lokalen Host verbunden sind, z. B. Loopback-, Ethernet-, ISDN-, PPP- oder Dummy-Geräte. In diese Spalte muss der Gerätename eingegeben werden.

In einer (optionalen) fünften Spalte kann der Typ einer Route angegeben werden. Nicht benötigte Spalten sollten ein Minuszeichen - enthalten, um sicherzustellen, dass der Parser den Befehl korrekt interpretiert. Weitere Informationen hierzu finden Sie auf der man-Seite für den Befehl `routes(5)`.

Das vereinheitlichte Format für IPv4 und IPv6 sieht nun wie folgt aus:

```
prefix/lengthgateway -            [interface]
```

Das so genannte Kompatibilitätsformat lautet entsprechend:

```
prefixgatewaylength       [interface]
```

Für IPv4 können Sie noch das alte Format mit Netzmaske verwenden:

```
ipv4-networkgatewayipv4-netmask [interface]
```

Die folgenden Beispiele sind Entsprechungen:

```
2001:db8:abba:cafe::/64 2001:db8:abba:cafe::dead  -             eth0
208.77.188.0/24         208.77.188.166            -             eth0

2001:db8:abba:cafe::    2001:db8:abba:cafe::dead 64             eth0
208.77.188.0            208.77.188.166           24             eth0

208.77.188.0            208.77.188.166           255.255.255.0 eth0
```

23.6.1.4 /etc/resolv.conf

In dieser Datei wird die Domäne angegeben, zu der der Host gehört (Schlüsselwort `search`). Ebenfalls aufgeführt ist der Status des Namenservers, auf den der Zugriff erfolgt (Schlüsselwort `nameserver`). In der Datei können mehrere Domänennamen angegeben werden. Bei der Auflösung eines Namens, der nicht voll qualifiziert ist, wird versucht, einen solchen zu generieren, indem die einzelnen `search`-Einträge angehängt werden. Mehrere Namenserver können in mehreren Zeilen angegeben werden, von denen jede mit `nameserver` beginnt. Kommentaren werden `#`-Zeichen vorangestellt. Beispiel 23.5, „/etc/resolv.conf“ (S. 367) zeigt, wie `/etc/resolv.conf` aussehen könnte.

Jedoch darf `/etc/resolv.conf` nicht manuell bearbeitet werden. Stattdessen wird es vom Skript `netconfig` generiert. Um die statische DNS-Konfiguration ohne YaST zu definieren, bearbeiten Sie die entsprechenden Variablen in der Datei `/etc/sysconfig/network/config` manuell:

`NETCONFIG_DNS_STATIC_SEARCHLIST`
: Liste der DNS-Domänennamen, die für die Suche nach Hostname verwendet wird

`NETCONFIG_DNS_STATIC_SERVERS`
: Liste der IP-Adressen des Nameservers, die für die Suche nach Hostname verwendet wird

`NETCONFIG_DNS_FORWARDER`
: Definiert den Namen des zu konfigurierenden DNS-Forwarders

Zum Deaktivieren der DNS-Konfiguration mit netconfig setzen Sie `NETCONFIG_DNS_POLICY=''`. Weitere Informationen über `netconfig` finden Sie auf `man 8 netconfig`.

Beispiel 23.5 */etc/resolv.conf*

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as name server
nameserver 192.168.1.116
```

23.6.1.5 /sbin/netconfig

`netconfig` ist ein modulares Tool zum Verwalten zusätzlicher Netzwerkkonfigurationseinstellungen. Es führt statisch definierte Einstellungen mit Einstellungen zusammen, die von automatischen Konfigurationsmechanismen wie DHCP oder PPP gemäß einer vordefinierten Richtlinie bereitgestellt wurden. Die erforderlichen Änderungen werden dem System zugewiesen, indem die netconfig-Module aufgerufen werden, die für das Ändern einer Konfigurationsdatei und den Neustart eines Service oder eine ähnliche Aktion verantwortlich sind.

`netconfig` erkennt drei Hauptaktionen. Die Kommandos `netconfig modify` und `netconfig remove` werden von Daemons wie DHCP oder PPP verwendet, um Einstellungen für netconfig hinzuzufügen oder zu entfernen. Nur das Kommando `netconfig update` steht dem Benutzer zur Verfügung:

`modify`
: Das Kommando `netconfig modify` ändert die aktuelle Schnittstellen- und Service-spezifischen dynamischen Einstellungen und aktualisiert die Netzwerkkonfiguration. Netconfig liest Einstellungen aus der Standardeingabe oder einer Datei, die mit der Option `--lease-file` *`Dateiname`* angegeben wurde, und speichert sie intern bis zu einem System-Reboot oder der nächsten Änderungs- oder Löschaktion). Bereits vorhandene Einstellungen für dieselbe Schnittstellen- und Service-Kombination werden überschrieben. Die Schnittstelle wird durch den Parameter `-i` *`Schnittstellenname`* angegeben. Der Service wird durch den Parameter `-s` *`Servicename`* angegeben.

`Entfernen`
: Das Kommando `netconfig remove` entfernt die dynamischen Einstellungen, die von einer Änderungsaktion für die angegebene Schnittstellen- und Service-Kombination bereitgestellt wurden, und aktualisiert die Netzwerkkonfiguration. Die Schnittstelle wird durch den Parameter `-i` *`Schnittstellenname`* angegeben. Der Service wird durch den Parameter `-s` *`Servicename`* angegeben.

`Aktualisieren`
: Das Kommando `netconfig update` aktualisiert die Netzwerkkonfiguration mit den aktuellen Einstellungen. Dies ist nützlich, wenn sich die Richtlinie oder die statische Konfiguration geändert hat. Verwenden Sie den Parameter `-m` *`Modultyp`*, wenn nur ein angegebener Dienst aktualisiert werden soll (`dns`,`nis` oder `ntp`).

Die Einstellungen für die netconfig-Richtlinie und die statische Konfiguration werden entweder manuell oder mithilfe von YaST in der Datei `/etc/sysconfig/network/config` definiert. Die dynamischen Konfigurationseinstellungen von Tools zur automatischen Konfiguration wie DHCP oder PPP werden von diesen Tools mit den Aktionen `netconfig modify` und `netconfig remove` direkt bereitgestellt. NetworkManager verwendet auch die Aktionen `netconfig modify` und `netconfig remove`. Wenn NetworkManager aktiviert ist, verwendet netconfig (im Richtlinienmodus `auto`) nur NetworkManager-Einstellungen und ignoriert Einstellungen von allen anderen Schnittstellen, die mit der traditionellen ifup-Methode konfiguriert wurden. Wenn NetworkManager keine Einstellung liefert, werden als Fallback statische Einstellungen verwendet. Eine gemischte Verwendung von NetworkManager und der traditionellen ifup-Methode wird nicht unterstützt.

Weitere Informationen über `netconfig` finden Sie auf `man 8 netconfig`.

23.6.1.6 /etc/hosts

In dieser Datei werden, wie in Beispiel 23.6, „`/etc/hosts`“ (S. 369) gezeigt, IP-Adressen zu Hostnamen zugewiesen. Wenn kein Namenserver implementiert ist, müssen alle Hosts, für die IP-Verbindungen eingerichtet werden sollen, hier aufgeführt sein. Geben Sie für jeden Host in die Datei eine Zeile ein, die aus der IP-Adresse, dem voll qualifizierten Hostnamen und dem Hostnamen besteht. Die IP-Adresse muss am Anfang der Zeile stehen und die Einträge müssen durch Leerzeichen und Tabulatoren getrennt werden. Kommentaren wird immer das `#`-Zeichen vorangestellt.

Beispiel 23.6 */etc/hosts*

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

23.6.1.7 /etc/networks

Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen. Weitere Informationen hierzu finden Sie unter Beispiel 23.7, „`/etc/networks`“ (S. 369).

Beispiel 23.7 */etc/networks*

```
loopback     127.0.0.0
localnet     192.168.0.0
```

23.6.1.8 /etc/host.conf

Das Auflösen von Namen, d. h. das Übersetzen von Host- bzw. Netzwerknamen über die *resolver*-Bibliothek, wird durch diese Datei gesteuert. Diese Datei wird nur für Programme verwendet, die mit libc4 oder libc5 gelinkt sind. Weitere Informationen zu aktuellen glibc-Programmen finden Sie in den Einstellungen in `/etc/nsswitch.conf`. Jeder Parameter muss in einer eigenen Zeile stehen. Kommentare werden durch ein `#`-Zeichen eingeleitet. Die verfügbaren Parameter sind in Tabelle 23.6, „Parameter für /etc/host.conf“ (S. 370) aufgeführt. Ein Beispiel für `/etc/host.conf` wird in Beispiel 23.8, „`/etc/host.conf`“ (S. 370) gezeigt.

Tabelle 23.6 Parameter für /etc/host.conf

order *hosts*, *bind*	Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente (getrennt durch Leerzeichen oder Kommas):
	Hosts: Sucht die `/etc/hosts`-Datei
	bind: Greift auf einen Namenserver zu
	nis: Verwendet NIS
multi *on*/*off*	Legt fest, ob ein in `/etc/hosts` eingegebener Host mehrere IP-Adressen haben kann.
nospoof *on* spoofalert *on*/*off*	Diese Parameter beeinflussen das *spoofing* des Namenservers, haben aber keinen Einfluss auf die Netzwerkkonfiguration.
trim *Domänenname*	Der angegebene Domänenname wird vor dem Auflösen des Hostnamens von diesem abgeschnitten (insofern der Hostname diesen Domänennamen enthält). Diese Option ist nur dann von Nutzen, wenn in der Datei `/etc/hosts` nur Namen aus der lokalen Domäne stehen, diese aber auch mit angehängtem Domänennamen erkannt werden sollen.

***Beispiel 23.8** /etc/host.conf*

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

23.6.1.9 /etc/nsswitch.conf

Mit der GNU C Library 2.0 wurde *Name Service Switch* (NSS) eingeführt. Weitere Informationen hierzu finden Sie auf der man-Seite für `nsswitch.conf(5)` und im Dokument *The GNU C Library Reference Manual.*

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Beispiel für `nsswitch.conf` ist in Beispiel 23.9, „`/etc/nsswitch.conf`“ (S. 371) dargestellt. Kommentaren werden `#`-Zeichen vorangestellt. Der Eintrag unter der `hosts`-Datenbank bedeutet, dass Anfragen über DNS an `/etc/hosts` (`files`) gehen.

Beispiel 23.9 */etc/nsswitch.conf*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files
rpc:        files
ethers:     files
netmasks:   files
netgroup:   files nis
publickey:  files

bootparams: files
automount:  files nis
aliases:    files nis
shadow:     compat
```

Die über NSS verfügbaren „Datenbanken“ sind in Tabelle 23.7, „Über /etc/nsswitch.conf verfügbare Datenbanken“ (S. 371) aufgelistet. Die Konfigurationsoptionen für NSS-Datenbanken sind in Tabelle 23.8, „Konfigurationsoptionen für NSS-„Datenbanken““ (S. 373) aufgelistet.

Tabelle 23.7 *Über /etc/nsswitch.conf verfügbare Datenbanken*

`aliases`	Mail-Aliasse, die von `sendmail` implementiert werden. Siehe `man5 aliases`.

ethers	Ethernet-Adressen
Netzmasken	Liste von Netzwerken und ihrer Teilnetzmasken. Wird nur benötigt, wenn Sie Subnetting nutzen.
Gruppe	Für Benutzergruppen, die von getgrent verwendet werden. Weitere Informationen hierzu finden Sie auch auf der man-Seite für den Befehl group.
hosts	Für Hostnamen und IP-Adressen, die von gethostbyname und ähnlichen Funktionen verwendet werden.
netgroup	Im Netzwerk gültige Host- und Benutzerlisten zum Steuern von Zugriffsrechten. Weitere Informationen hierzu finden Sie auf der man-Seite für netgroup(5).
networks	Netzwerknamen und -adressen, die von getnetent verwendet werden.
publickey	Öffentliche und geheime Schlüssel für Secure_RPC, verwendet durch NFS and NIS+.
passwd	Benutzerpasswörter, die von getpwent verwendet werden. Weitere Informationen hierzu finden Sie auf der man-Seite passwd(5).
protocols	Netzwerkprotokolle, die von getprotoent verwendet werden. Weitere Informationen hierzu finden

	Sie auf der man-Seite für `protocols(5)`.
`rpc`	Remote Procedure Call-Namen und -Adressen, die von `getrpcbyname` und ähnlichen Funktionen verwendet werden.
`services`	Netzwerkdienste, die von `getservent` verwendet werden.
`shadow`	Shadow-Passwörter der Benutzer, die von `getspnam` verwendet werden. Weitere Informationen hierzu finden Sie auf der man-Seite für `shadow(5)`.

***Tabelle 23.8** Konfigurationsoptionen für NSS-„Datenbanken“*

`Dateien`	Direkter Dateizugriff, z. B. `/etc/aliases`
`db`	Zugriff über eine Datenbank
`nis`, `nisplus`	NIS, siehe auch Chapter 3, *Using NIS* (↑*Security Guide*)
`dns`	Nur bei `hosts` und `networks` als Erweiterung verwendbar
`compat`	Nur bei `passwd`, `shadow` und `group` als Erweiterung verwendbar

23.6.1.10 /etc/nscd.conf

Mit dieser Datei wird nscd (Name Service Cache Daemon) konfiguriert. Weitere Informationen hierzu finden Sie auf den man-Seiten `nscd(8)` und `nscd.conf(5)`. Standardmäßig werden die Systemeinträge von `passwd` und `groups` von nscd gecacht.

Dies ist wichtig für die Leistung der Verzeichnisdienste, z. B. NIS und LDAP, da anderenfalls die Netzwerkverbindung für jeden Zugriff auf Namen oder Gruppen verwendet werden muss. `hosts` wird standardmäßig nicht gecacht, da der Mechanismus in nscd dazu führen würde, dass das lokale System keine Trust-Forward- und Reverse-Lookup-Tests mehr ausführen kann. Statt nscd das Cachen der Namen zu übertragen, sollten Sie einen DNS-Server für das Cachen einrichten.

Wenn das Caching für `passwd` aktiviert wird, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten von nscd mit dem Befehl `rcnscd restart` kann diese Wartezeit verkürzt werden.

23.6.1.11 /etc/HOSTNAME

Diese Datei enthält den voll qualifizierten Hostnamen mit angehängtem Domänennamen. Diese Datei wird von verschiedenen Skripten beim Booten des Computers gelesen. Sie darf nur eine Zeile enthalten (in der der Hostname festgelegt ist).

23.6.2 Testen der Konfiguration

Bevor Sie Ihre Konfiguration in den Konfigurationsdateien speichern, können Sie sie testen. Zum Einrichten einer Testkonfiguration verwenden Sie den Befehl `ip`. Zum Testen der Verbindung verwenden Sie den Befehl `ping`. Ältere Konfigurationswerkzeuge, `ifconfig` und `route`, sind ebenfalls verfügbar.

Die Kommandos `ip`, `ifconfig` und `route` ändern die Netzwerkkonfiguration direkt, ohne sie in der Konfigurationsdatei zu speichern. Wenn Sie die Konfiguration nicht in die korrekten Konfigurationsdateien eingeben, geht die geänderte Netzwerkkonfiguration nach dem Neustart verloren.

23.6.2.1 Konfigurieren einer Netzwerkschnittstelle mit ip

`ip` ist ein Werkzeug zum Anzeigen und Konfigurieren von Netzwerkgeräten, Richtlinien-Routing und Tunneln.

`ip` ist ein sehr komplexes Werkzeug. Seine allgemeine Syntax ist `ip` *`options object command`*. Sie können mit folgenden Objekten arbeiten:

Verbindung
: Dieses Objekt stellt ein Netzwerkgerät dar.

Adresse
: Dieses Objekt stellt die IP-Adresse des Geräts dar.

Nachbar
: Dieses Objekt stellt einen ARP- oder NDISC-Cache-Eintrag dar.

route
: Dieses Objekt stellt den Routing-Tabelleneintrag dar.

Regel
: Dieses Objekt stellt eine Regel in der Routing-Richtlinien-Datenbank dar.

maddress
: Dieses Objekt stellt eine Multicast-Adresse dar.

mroute
: Dieses Objekt stellt einen Multicast-Routing-Cache-Eintrag dar.

tunnel
: Dieses Objekt stellt einen Tunnel über IP dar.

Wird kein Kommando angegeben, wird das Standardkommando verwendet (normalerweise `list`).

Ändern Sie den Gerätestatus mit dem Befehl `ip link set` *`device_name command`*. Wenn Sie beispielsweise das Gerät eth0 deaktivieren möchten, geben Sie `ip link seteth0 down ein`. Um es wieder zu aktivieren, verwenden Sie `ip link seteth0 up`.

Nach dem Aktivieren eines Geräts können Sie es konfigurieren. Verwenden Sie zum Festlegen der IP-Adresse `ip addr add`*`ip_address`*` + dev `*`device_name`*. Wenn Sie beispielsweise die Adresse der Schnittstelle eth0 mit dem standardmäßigen Broadcast (Option `brd`) auf 192.168.12.154/30 einstellen möchten, geben Sie `ip addr add 192.168.12.154/30 brd + dev eth0` ein.

Damit die Verbindung funktioniert, müssen Sie außerdem das Standard-Gateway konfigurieren. Geben Sie `ip route add gateway_ip_address` ein, wenn Sie ein Gateway für Ihr System festlegen möchten. Um eine IP-Adresse in eine andere Adresse

zu übersetzen, verwenden Sie `nat`: `ip route add nat ip_address via other_ip_address`.

Zum Anzeigen aller Geräte verwenden Sie `ip link ls`. Wenn Sie nur die aktiven Schnittstellen abrufen möchten, verwenden Sie `ip link ls up`. Um Schnittstellenstatistiken für ein Gerät zu drucken, geben Sie `ip -s link lsdevice_name` ein. Um die Adressen Ihrer Geräte anzuzeigen, geben Sie `ip addr` ein. In der Ausgabe von `ip addr` finden Sie auch Informationen zu MAC-Adressen Ihrer Geräte. Wenn Sie alle Routen anzeigen möchten, wählen Sie `ip route show`.

Weitere Informationen zur Verwendung von `ip` erhalten Sie, indem Sie `iphelp` eingeben oder die man-Seite `ip(8)` aufrufen. Die Option `help` ist zudem für alle `ip`-Unterkommandos verfügbar. Wenn Sie beispielsweise Hilfe zu `ipaddr` benötigen, geben Sie `ipaddr help` ein. Suchen Sie die `ip`-Manualpage in der Datei `/usr/share/doc/packages/iproute2/ip-cref.pdf`.

23.6.2.2 Testen einer Verbindung mit ping

Der `ping`-Befehl ist das Standardwerkzeug zum Testen, ob eine TCP/IP-Verbindung funktioniert. Er verwendet das ICMP-Protokoll, um ein kleines Datenpaket, das ECHO_REQUEST-Datagram, an den Ziel-Host zu senden. Dabei wird eine sofortige Antwort angefordert. Funktioniert dies, wird von `ping` eine Meldung angezeigt, die Ihnen bestätigt, dass die Netzwerkverbindung grundsätzlich funktioniert.

`ping` testet nicht nur die Funktion der Verbindung zwischen zwei Computern, es bietet darüber hinaus grundlegende Informationen zur Qualität der Verbindung. In Beispiel 23.10, „Ausgabe des ping-Befehls“ (S. 377) sehen Sie ein Beispiel der `ping`-Ausgabe. Die vorletzte Zeile enthält Informationen zur Anzahl der übertragenen Pakete, der verlorenen Pakete und der Gesamtlaufzeit von `ping`.

Als Ziel können Sie einen Hostnamen oder eine IP-Adresse verwenden, z. B. `ping example.com` oder `ping 192.168.3.100`. Das Programm sendet Pakete, bis Sie auf Strg + C drücken.

Wenn Sie nur die Funktion der Verbindung überprüfen möchten, können Sie die Anzahl der Pakete durch die Option `-c` beschränken. Wenn Sie die Anzahl beispielsweise auf drei Pakete beschränken möchten, geben Sie `ping -c 3 example.com` ein.

Beispiel 23.10 *Ausgabe des ping-Befehls*

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

Das Standardintervall zwischen zwei Paketen beträgt eine Sekunde. Zum Ändern des Intervalls bietet das ping-Kommando die Option `-i`. Wenn beispielsweise das Ping-Intervall auf zehn Sekunden erhöht werden soll, geben Sie `ping -i 10 example.com` ein.

In einem System mit mehreren Netzwerkgeräten ist es manchmal nützlich, wenn der ping-Befehl über eine spezifische Schnittstellenadresse gesendet wird. Verwenden Sie hierfür die Option `-I` mit dem Namen des ausgewählten Geräts. Beispiel: `ping -I wlan1 example.com`.

Weitere Optionen und Informationen zur Verwendung von ping erhalten Sie, indem Sie `ping-h` eingeben oder die man-Seite `ping (8)` aufrufen.

TIPP: Ping-Ermittlung für IPv6-Adressen

Verwenden Sie für IPv6-Adressen das Kommando `ping6`. Hinweis: Zur Ping-Ermittlung für Link-Local-Adressen müssen Sie die Schnittstelle mit `-I` angeben. Das folgende Kommando funktioniert, wenn die Adresse über `eth1` erreichbar ist:

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

23.6.2.3 Konfigurieren des Netzwerks mit dem ifconfig-Befehl

`ifconfig` ist ein Werkzeug zur Netzwerkkonfiguration.

ANMERKUNG: ifconfig und ip

Das `ifconfig`-Werkzeug ist veraltet. Verwenden Sie stattdessen `ip`. Im Gegensatz zu `ip` können Sie `ifconfig` nur für die Schnittstellenkonfiguration verwenden. Schnittstellennamen sind damit auf 9 Zeichen beschränkt.

Ohne Argumente zeigt `ifconfig` den Status der gegenwärtig aktiven Schnittstellen an. Unter Beispiel 23.11, „Ausgabe des `ifconfig`-Kommandos“ (S. 378) sehen Sie, dass `ifconfig` über eine gut angeordnete, detaillierte Ausgabe verfügt. Die Ausgabe enthält außerdem in der ersten Zeile Informationen zur MAC-Adresse Ihres Geräts (dem Wert von `HWaddr`).

Beispiel 23.11 *Ausgabe des ifconfig-Kommandos*

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 MB)
```

Weitere Optionen und Informationen zur Verwendung von `ifconfig` erhalten Sie, wenn Sie `ifconfig -h` eingeben oder die man-Seite `ifconfig (8)` aufrufen.

23.6.2.4 Konfigurieren des Routing mit route

route ist ein Programm zum Ändern der IP-Routing-Tabelle. Sie können damit Ihre Routing-Konfiguration anzeigen und Routen hinzufügen oder entfernen.

ANMERKUNG: route und ip

Das route-Programm ist veraltet. Verwenden Sie stattdessen ip.

---

route ist vor allem dann nützlich, wenn Sie schnelle und übersichtliche Informationen zu Ihrer Routing-Konfiguration benötigen, um Routing-Probleme zu ermitteln. Sie sehen Ihre aktuelle Routing-Konfiguration unter route-n als root.

Beispiel 23.12 *Ausgabe des route -n-Kommandos*

```
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.20.0.0       *               255.255.248.0   U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
loopback        *               255.0.0.0       U         0 0          0 lo
default         styx.exam.com   0.0.0.0         UG        0 0          0 eth0
```

Weitere Optionen und Informationen zur Verwendung von route erhalten Sie, indem Sie -h eingeben oder die man-Seite route (8) aufrufen.

23.6.3 Startup-Skripten

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripten, die beim Booten des Computers die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Mehrbenutzer-Runlevel* wechselt. Einige der Skripten sind in Tabelle 23.9, „Einige Start-Skripten für Netzwerkprogramme“ (S. 379) beschrieben.

Tabelle 23.9 *Einige Start-Skripten für Netzwerkprogramme*

/etc/init.d/network	Dieses Skript übernimmt die Konfiguration der Netzwerkschnittstellen. Wenn der Netzwerkdienst nicht

	gestartet wurde, werden keine Netzwerkschnittstellen implementiert.
/etc/init.d/xinetd	Startet xinetd. Mit xinetd können Sie Serverdienste auf dem System verfügbar machen. Beispielsweise kann er vsftpd starten, sobald eine FTP-Verbindung initiiert wird.
/etc/init.d/rpcbind	Startet das rpcbind-Dienstprogramm, das RPC-Programmnummern in universelle Adressen konvertiert. Es ist für RPC-Dienste wie NFS-Server erforderlich.
/etc/init.d/nfsserver	Startet den NFS-Server.
/etc/init.d/postfix	Steuert den postfix-Prozess.
/etc/init.d/ypserv	Startet den NIS-Server.
/etc/init.d/ypbind	Startet den NIS-Client.

23.7 Einrichten von Bonding-Geräten

Für bestimmte Systeme sind Netzwerkverbindungen erforderlich, die die normalen Anforderungen an die Datensicherheit oder Verfügbarkeit von typischen Ethernet-Geräten übertreffen. In diesen Fällen lassen sich mehrere Ethernet-Geräte zu einem einzigen Bonding-Gerät zusammenschließen.

Die Konfiguration des Bonding-Geräts erfolgt dabei über die Bonding-Moduloptionen. Das Verhalten ergibt sich im wesentlichen aus dem Modus des Bonding-Geräts. Standardmäßig gilt `mode=active-backup`; wenn das aktive Slave-Gerät ausfällt, wird also ein anderes Slave-Gerät aktiviert.

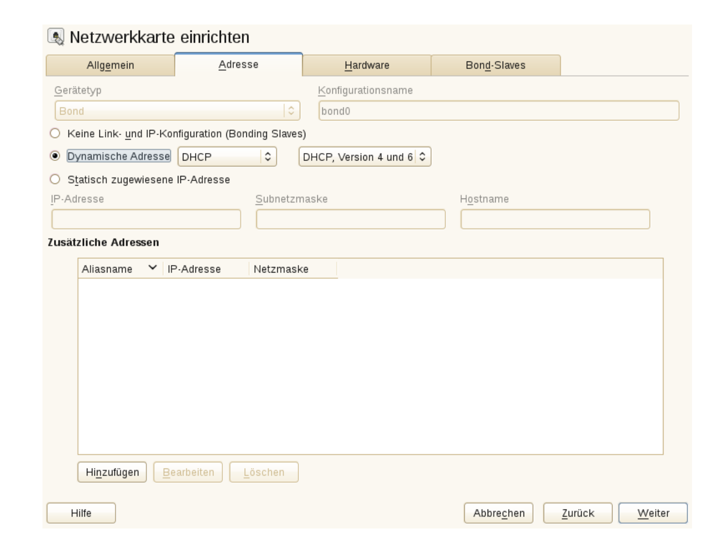
TIPP: Bonding und Xen

Der Einsatz von Bonding-Geräten empfiehlt sich nur für Computer, in denen mehrere physische Netzwerkkarten eingebaut sind. Bei den meisten Konstellationen sollten Sie die Bonding-Konfiguration daher lediglich in Domain0 verwenden. Die Bond-Einrichtung in einem VM-Gast-System ist dabei nur dann sinnvoll, wenn dem VM-Gast mehrere Netzwerkkarten zugewiesen sind.

Zum Konfigurieren eines Bonding-Geräts gehen Sie wie folgt vor:

1 Führen Sie *YaST* > *Netzwerkgeräte* > *Netzwerkeinstellungen* aus.

2 Wählen Sie *Hinzufügen* und ändern Sie die Einstellung unter *Gerätetyp* in *Bond*. Fahren Sie mit *Weiter* fort.



3 Geben Sie an, wie dem Bonding-Gerät eine IP-Adresse zugewiesen werden soll. Hierfür stehen drei Methoden zur Auswahl:

- No IP Address (Keine IP-Adresse)
- Dynamic Address (with DHCP or Zeroconf) (Dynamische Adresse (mit DHCP oder Zeroconf))

- Statisch zugewiesene IP-Adresse

Wählen Sie die passende Methode für Ihre Umgebung aus.

4. Wählen Sie auf dem Karteireiter *Bond-Slaves* die Ethernet-Geräte aus, die in den Bond aufgenommen werden sollen. Aktivieren Sie hierzu die entsprechenden Kontrollkästchen.

5. Bearbeiten Sie die Einstellungen unter *Bond-Treiberoptionen*. Für die Konfiguration stehen die folgenden Modi zur Auswahl:

   - balance-rr
   - active-backup
   - balance-xor
   - Rundsendung
   - 802.3ad
   - balance-tlb
   - balance-alb

6. Der Parameter `miimon=100` muss unter *Bond-Treiberoptionen* angegeben werden. Ohne diesen Parameter wird die Datenintegrität nicht regelmäßig überprüft.

7. Klicken Sie auf *Weiter*, und beenden Sie YaST mit *OK*. Das Gerät wird erstellt.

Alle Modi und viele weitere Optionen werden ausführlich im Dokument *Linux Ethernet Bonding Driver HOWTO* erläutert, das nach der Installation des Pakets `kernel-source` unter `/usr/src/linux/Documentation/networking/bonding.txt` verfügbar ist.

23.7.1 Hot-Plugging von Bonding-Slaves

In bestimmten Netzwerkumgebungen (z. B. High Availability) muss eine Bonding-Slave-Schnittstelle durch eine andere Schnittstelle ersetzt werden. Dieser Fall tritt bei-

spielsweise ein, wenn ein Netzwerkgerät wiederholt ausfällt. Die Lösung ist hier das Hot-Plugging der Bonding-Slaves.

Der Bond wird wie gewohnt konfiguriert (gemäß `man 5 ifcfg-bonding`), beispielsweise:

```
ifcfg-bond0
          STARTMODE='auto' # or 'onboot'
          BOOTPROTO='static'
          IPADDR='192.168.0.1/24'
          BONDING_MASTER='yes'
          BONDING_SLAVE_0='eth0'
          BONDING_SLAVE_1='eth1'
          BONDING_MODULE_OPTS='mode=active-backup miimon=100'
```

Die Slaves werden jedoch mit `STARTMODE=hotplug` und `BOOTPROTO=none` angegeben:

```
ifcfg-eth0
          STARTMODE='hotplug'
          BOOTPROTO='none'

ifcfg-eth1
          STARTMODE='hotplug'
          BOOTPROTO='none'
```

Bei `BOOTPROTO=none` werden die ethtool-Optionen herangezogen (sofern bereitgestellt), es wird jedoch kein Link zu `ifup eth0` eingerichtet. Dies ist darin begründet, dass die Slave-Schnittstelle durch den Bond-Master gesteuert wird.

Bei `STARTMODE=hotplug` wird die Slave-Schnittstelle dem Bond automatisch zugefügt, sobald diese verfügbar ist.

Die `udev`-Regeln unter `/etc/udev/rules.d/70-persistent-net.rules` müssen so geändert werden, dass das Gerät über die Bus-ID (udev-Schlüsselwort `KERNELS` „SysFS BusID“ wie in `hwinfo --netcard`) statt über die MAC-Adresse angesteuert wird, damit fehlerhafte Hardware ausgetauscht werden kann (Netzwerkkarte im gleichen Steckplatz, jedoch mit anderer MAC) und Verwirrung vermieden wird, da der Bond die MAC-Adresse aller Slaves ändert.

Beispiel:

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
```

```
KERNELS=="0000:00:19.0", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"
```

Beim Booten wartet `/etc/init.d/network` nicht darauf, dass die Hot-Plug-Slaves einsatzbereit sind, sondern es wird die Bereitschaft des gesamten Bonds abgewartet, wofür mindestens ein verfügbarer Slave erforderlich ist. Wenn eine Slave-Schnittstelle aus dem System entfernt wird (durch Aufheben der Bindung an den NIC-Treiber, durch `rmmod` des NIC-Treibers oder durch normales PCI-Hot-Plug-Entfernen), so entfernt der Kernel die betreffende Schnittstelle automatisch aus dem Bond. Wird eine neue Karte in das System eingebaut (Austausch der Hardware im Steckplatz), benennt `udev` diese Karte anhand der Regel für busgestützte permanente Namen in den Namen des Slaves um und ruft `ifup` für die Karte auf. Mit dem `ifup`-Aufruf tritt die Karte automatisch in den Bond ein.

23.8 smpppd als Einwählhelfer

Einige Heimanwender besitzen keine gesonderte Leitung für das Internet, sondern wählen sich bei Bedarf ein. Je nach Einwählart (ISDN oder DSL) wird die Verbindung von ipppd oder pppd gesteuert. Im Prinzip müssen nur diese Programme korrekt gestartet werden, um online zu sein.

Sofern Sie über eine Flatrate verfügen, die bei der Einwahl keine zusätzlichen Kosten verursacht, starten Sie einfach den entsprechenden Daemon. Sie können die Einwählverbindung über ein Desktop-Miniprogramm oder eine Kommandozeilen-Schnittstelle steuern. Wenn das Internet-Gateway nicht der eigentliche Arbeitscomputer ist, besteht die Möglichkeit, die Einwählverbindung über einen Host im Netzwerk zu steuern.

Hier kommt smpppd (SUSE Meta PPP Daemon) ins Spiel. Der Dienst bietet den Hilfsprogrammen eine einheitliche Schnittstelle, die in zwei Richtungen funktioniert. Zum einen programmiert er den jeweils erforderlichen pppd oder ipppd und steuert deren Einwählverhalten. Zum anderen stellt er den Benutzerprogrammen verschiedene Provider zur Verfügung und übermittelt Informationen zum aktuellen Status der Verbindung. Da der smpppd-Dienst auch über das Netzwerk gesteuert werden kann, eignet er sich für die Steuerung von Einwählverbindungen ins Internet von einer Arbeitsstation in einem privaten Subnetzwerk.

23.8.1 Konfigurieren von smpppd

Die von smpppd bereitgestellten Verbindungen werden automatisch von YaST konfiguriert. Die eigentlichen Einwählprogramme KInternet und cinternet werden ebenfalls vorkonfiguriert. Manuelle Einstellungen sind nur notwendig, wenn Sie zusätzliche Funktionen von smpppd, z. B. die Fernsteuerung, einrichten möchten.

Die Konfigurationsdatei von smpppd ist `/etc/smpppd.conf`. Sie ist so eingestellt, dass standardmäßig keine Fernsteuerung möglich ist. Die wichtigsten Optionen dieser Konfigurationsdatei sind:

open-inet-socket = *`yes|no`*
: Zur Steuerung von smpppd über das Netzwerk stellen Sie diese Option auf `yes` (ja) ein. smpppd überwacht Port `3185`. Wenn dieser Parameter auf `yes` (ja) gesetzt ist, müssen auch die Parameter `bind-address`, `host-range` und `password` entsprechend eingestellt werden.

bind-address = *`IP-Adresse`*
: Wenn ein Host mehrere IP-Adressen hat, können Sie mit dieser Einstellung festlegen, über welche IP-Adresse smpppd Verbindungen akzeptiert. Standard ist die Überwachung an allen Adressen.

host-range = *`Anfangs-IPEnd-IP`*
: Der Parameter `host-range` definiert einen Netzbereich. Hosts, deren IP-Adressen innerhalb dieses Bereichs liegen, wird der Zugriff auf smpppd gewährt. Alle Hosts, die außerhalb dieses Bereichs liegen, werden abgewiesen.

password = *`Passwort`*
: Mit der Vergabe eines Passworts wird der Client-Zugriff auf autorisierte Hosts beschränkt. Da es lediglich ein reines Textpasswort ist, sollte die Sicherheit, die es bietet, nicht überbewertet werden. Wenn kein Passwort vergeben wird, sind alle Clients berechtigt, auf smpppd zuzugreifen.

slp-register = *`yes|no`*
: Mit diesem Parameter kann der smpppd-Dienst per SLP im Netzwerk bekannt gegeben werden.

Weitere Informationen zu smpppd finden Sie in den man-Seiten zu `smpppd(8)` und `smpppd.conf(5)`.

23.8.2 Konfigurieren von cinternet für die Remote-Verwendung

cinternet kann zur Steuerung eines lokalen oder entfernten smpppd-Dienstes verwendet werden. cinternet mit Kommandozeilen ist das Gegenstück zum grafischen KInternet. Wenn Sie diese Dienstprogramme zum Einsatz mit einem entfernten smpppd-Dienst vorbereiten möchten, bearbeiten Sie die Konfigurationsdatei `/etc/smpppd-c.conf` manuell oder mithilfe von cinternet. Diese Datei enthält nur vier Optionen:

sites = *`Liste der Sites`*
: *`Liste der Sites`*, an denen die Frontends nach smpppd suchen. Die Frontends testen die Optionen in der hier angegebenen Reihenfolge. `Lokal` verlangt den Verbindungsaufbau zum lokalen smpppd. `Gateway` verweist auf ein smpppd am Gateway. `config-file` gibt an, dass die Verbindung zum smpppd hergestellt werden sollte, der in den Optionen `Server` und `Port` in der Datei `/etc/smpppd-c.conf` angegeben ist. `slp` veranlasst, dass die Front-Ends eine Verbindung zu einem über SLP gefundenen smpppd aufbauen.

server = *`Server`*
: Der Host, auf dem smpppd ausgeführt wird.

Port = *`Port`*
: Der Port, auf dem smpppd ausgeführt wird.

password = *`Passwort`*
: Das Passwort, das für smpppd ausgewählt wurde.

Wenn smpppd aktiv ist, versuchen Sie, darauf zuzugreifen. Verwenden Sie dazu beispielsweise `cinternet --verbose --interface-list`. Sollten Sie an dieser Stelle Schwierigkeiten haben, finden Sie weitere Informationen in den man-Seiten zu `smpppd-c.conf(5)` und `cinternet(8)`.

24 SLP-Dienste im Netzwerk

Das *Service Location Protocol* (SLP) wurde entwickelt, um die Konfiguration vernetzter Clients innerhalb eines lokalen Netzwerks zu vereinfachen. Zur Konfiguration eines Netzwerk-Clients inklusive aller erforderlichen Dienste benötigt der Administrator traditionell detailliertes Wissen über die im Netzwerk verfügbaren Server. SLP teilt allen Clients im lokalen Netzwerk die Verfügbarkeit ausgewählter Dienste mit. Anwendungen mit SLP-Unterstützung können diese Informationen verarbeiten und können automatisch konfiguriert werden.

SUSE® Linux Enterprise Desktop unterstützt die Installation von per SLP bekannt gegebenen Installationsquellen und beinhaltet viele Systemdienste mit integrierter Unterstützung für SLP. YaST und Konqueror verfügen beide über SLP-fähige Frontends. Nutzen Sie SLP, um vernetzten Clients zentrale Funktionen wie Installationsserver, YOU-Server, Dateiserver oder Druckserver auf Ihrem System zur Verfügung zu stellen.

WICHTIG: SLP-Unterstützung in SUSE Linux Enterprise Desktop

Dienste, die SLP-Unterstützung bieten, sind u. a. cupsd, rsyncd, ypserv, openldap2, ksysguardd, saned, kdm, vnc, login, smpppd, rpasswd, postfix und sshd (über fish).

24.1 Installation

Alle erforderlichen Pakete werden standardmäßig installiert. Falls Sie jedoch Dienste via SLP bereitstellen möchten, müssen Sie sicherstellen, dass auch das Paket `openslp-server` installiert wird.

24.2 SLP aktivieren

slpd muss auf Ihrem System ausgeführt werden, damit Dienste mit SLP angeboten werden können. Wenn der Computer nur als Client fungieren soll und keine Dienste anbietet, ist es nicht erforderlich, slpd auszuführen. Wie die meisten Systemdienste unter SUSE Linux Enterprise Desktop wird der slpd-Daemon über ein separates `init`-Skript gesteuert. Nach der Installation ist der Dämon standardmäßig inaktiv. Wenn Sie ihn temporär aktivieren möchten, führen Sie `rcslpd start` als `root` aus. Zum Stoppen führen Sie `rcslpd stop` aus. Mit `restart` oder `status` lösen Sie einen Neustart oder eine Statusabfrage aus. Wenn slpd nach dem Booten immer aktiv sein soll, aktivieren Sie slpd in YaST *System* > *Systemdienste (Runlevel)* oder führen Sie das Kommando `insserv slpd` als `root` aus.

24.3 SLP-Frontends in SUSE Linux Enterprise Desktop

Verwenden Sie für die Suche nach Diensten, die über SLP bereitgestellt werden, in Ihrem Netzwerk ein SLP-Frontend wie `slptool` (`openslp`-Paket) oder YaST:

slptool
: slptool ist ein Kommandozeilenprogramm, mit dem SLP-Abfragen im Netzwerk oder proprietäre Dienste bekannt gegeben werden können. Mit `slptool --help` werden alle verfügbaren Optionen und Funktionen aufgelistet. Um beispielsweise alle Zeitserver zu finden, die sich selbst im aktuellen Netzwerk bekannt geben, führen Sie folgendes Kommando aus:

```
slptool findsrvs service:ntp
```

YaST
: YaST stellt außerdem einen SLP-Browser zur Verfügung. Dieser Browser ist jedoch nicht über das YaST-Kontrollzentrum verfügbar. Führen Sie zum Starten dieses Browsers `yast2 slp` als `root`-Benutzer aus. Klicken Sie auf *Dienstarten* auf der linken Seite, um weitere Informationen zu einem Dienst zu erhalten.

24.4 Bereitstellen von Diensten über SLP

Viele Anwendungen unter SUSE Linux Enterprise Desktop verfügen durch die `libslp`-Bibliothek über eine integrierte SLP-Unterstützung. Falls ein Dienst ohne SLP-Unterstützung kompiliert wurde, können Sie ihn mit einer der folgenden Methoden per SLP verfügbar machen:

Statische Registrierung über `/etc/slp.reg.d`

Legen Sie für jeden neuen Dienst eine separate Registrierungsdatei an. Das folgende Beispiel veranschaulicht die Registrierung eines Scanner-Diensts:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

Die wichtigste Zeile dieser Datei ist die *Dienst-URL*, die mit `service:` beginnt. Sie enthält den Diensttyp (`scanner.sane`) und die Adresse, unter der der Dienst auf dem Server verfügbar ist. *`$HOSTNAME`* wird automatisch durch den vollständigen Hostnamen ersetzt. Abgetrennt durch einen Doppelpunkt folgt nun der Name des TCP-Ports, auf dem der entsprechende Dienst gefunden werden kann. Geben Sie nun die Sprache an, in der der Dienst angekündigt werden soll, und die Gültigkeitsdauer der Registrierung in Sekunden. Diese Angaben müssen durch Kommas von der Dienst-URL getrennt werden. Wählen Sie für die Registrierungsdauer einen Wert zwischen `0` und `65535`. `0` verhindert die Registrierung. `Mit` 65535 werden alle Einschränkungen aufgehoben.

Die Registrierungsdatei enthält außerdem die beiden Variablen `watch-port-tcp` und `description`. `watch-port-tcp` koppelt die SLP-Dienstankündigung daran, ob der entsprechende Dienst aktiv ist, indem slpd den Status des Diensts überprüft. Die zweite Variable enthält eine genauere Beschreibung des Diensts, die in den entsprechenden Browsern angezeigt wird.

Statische Registrierung über /etc/slp.reg
: Der einzige Unterschied zwischen dieser Methode und der Prozedur mit /etc/slp.reg.d besteht darin, dass alle Dienste in einer zentralen Datei gruppiert sind.

Dynamische Registrierung über slptool
: Wenn ein Dienst dynamisch ohne Verwendung von Konfigurationsdateien registriert werden soll, verwenden Sie das Kommandozeilenprogramm slptool. Dasselbe Programm kann auch die Registrierung eines bestehenden Dienstangebots aufheben, ohne slpd neu zu starten.

24.5 Weiterführende Informationen

RFC 2608, 2609, 2610
: RFC 2608 befasst sich mit der Definition von SLP im Allgemeinen. RFC 2609 geht näher auf die Syntax der verwendeten Dienst-URLs ein und RFC 2610 thematisiert DHCP über SLP.

http://www.openslp.org
: Die Homepage des OpenSLP-Projekts.

/usr/share/doc/packages/openslp
: Dieses Verzeichnis enthält die Dokumentation für SLP, die im Lieferumfang des openslp-server-Pakets enthalten ist, einschließlich einer README.SuSE-Datei mit den SUSE Linux Enterprise Desktop-Details, den RFCs und zwei einführenden HTML-Dokumenten. Programmierer, die an den SLP-Funktionen interessiert sind, finden weitere Informationen im *Programmierhandbuch*, das im Paket openslp-devel enthalten ist.

25 Zeitsynchronisierung mit NTP

Der NTP-(Network Time Protocol-)Mechanismus ist ein Protokoll für die Synchronisierung der Systemzeit über das Netzwerk. Erstens kann ein Computer die Zeit von einem Server abrufen, der als zuverlässige Zeitquelle gilt. Zweitens kann ein Computer selbst für andere Computer im Netzwerk als Zeitquelle fungieren. Es gibt zwei Ziele – das Aufrechterhalten der absoluten Zeit und das Synchronisieren der Systemzeit aller Computer im Netzwerk.

Das Aufrechterhalten der genauen Systemzeit ist in vielen Situationen wichtig. Die integrierte Hardware-Uhr erfüllt häufig nicht die Anforderungen bestimmter Anwendungen, beispielsweise Datenbanken oder Cluster. Die manuelle Korrektur der Systemzeit würde schwerwiegende Probleme nach sich ziehen; das Zurückstellen kann beispielsweise zu Fehlfunktionen wichtiger Anwendungen führen. Die Systemzeiten der in einem Netzwerk zusammengeschlossenen Computer müssen in der Regel synchronisiert werden. Es empfiehlt sich aber nicht, die Zeiten manuell anzugleichen. Vielmehr sollten Sie dazu NTP verwenden. Der NTP-Dienst passt die Systemzeit ständig anhand zuverlässiger Zeitserver im Netzwerk an. Zudem ermöglicht er die Verwaltung lokaler Referenzuhren, beispielsweise funkgesteuerter Uhren.

ANMERKUNG

Folgen Sie den Anweisungen unter Procedure “Joining an AD Domain” (↑*Security Guide*), um die Zeitsynchronisierung mithilfe von Active Directory zu aktivieren.

25.1 Konfigurieren eines NTP-Client mit YaST

Der NTP-Daemon (`ntpd`) im `ntp`-Paket ist so voreingestellt, dass die Uhr des lokalen Computers als Zeitreferenz verwendet wird. Das Verwenden der Hardware-Uhr ist jedoch nur eine Ausweichlösung, wenn keine genauere Zeitquelle verfügbar ist. YaST erleichtert die Konfiguration von NTP-Clients.

25.1.1 Grundlegende Konfiguration

Die NTP-Client-Konfiguration mit YaST (*Netzwerkdienste* > *NTP-Konfiguration*) benötigt zwei Dialogfelder. Legen Sie den Startmodus `ntpd` und den abzufragenden Server auf dem Karteireiter *Allgemein Einstellungen* fest.

Nur manuell
: Wählen Sie *Nur manuell*, wenn der `ntpd`-Daemon manuell gestartet werden soll.

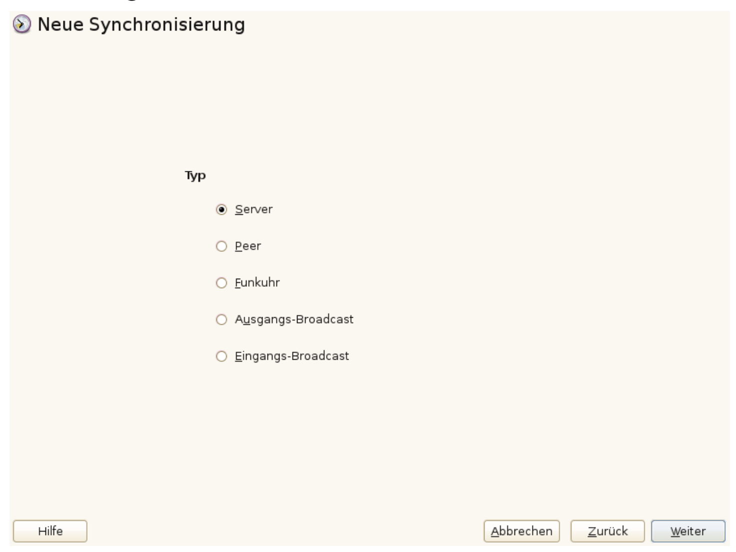
Jetzt und beim Booten
: Wählen Sie *Jetzt und beim Booten*, um `ntpd` automatisch beim Booten des Systems zu starten. Diese Einstellung wird dringend empfohlen. Konfigurieren Sie dann den Server entsprechend der Beschreibung Abschnitt 25.1.2, „Ändern der Basiskonfiguration“ (S. 392).

25.1.2 Ändern der Basiskonfiguration

Die Server und anderen Zeitquellen für die Abfrage durch den Client sind im unteren Bereich im Karteireiter *Allgemeine Einstellungen* aufgelistet. Bearbeiten Sie diese Liste nach Bedarf mithilfe der Optionen *Hinzufügen*, *Bearbeiten* und *Löschen*. *Mit* Protokoll anzeigen können die Protokolldateien Ihres Clients angezeigt werden.

Klicken Sie auf *Hinzufügen*, um eine neue Quelle für Zeitinformationen hinzuzufügen. Wählen Sie im nachfolgenden Dialogfeld den Quellentyp aus, mit dem die Zeitsynchronisierung vorgenommen werden soll. Mit den zur Verfügung stehenden Optionen können Sie

Abbildung 25.1 *YaST: NTP-Server*



Server
: Geben Sie in der Pulldown-Liste unter *Auswählen* (siehe Abbildung 25.1, „YaST: NTP-Server" (S. 393)) an, ob die Zeitsynchronisierung anhand eines Zeitservers in Ihrem lokalen Netzwerk (*Lokaler NTP-Server*) oder eines Zeitservers im Internet erfolgen soll, der Ihre Zeitzone verwaltet (*Öffentlicher NTP-Server*). Bei einem lokalen Zeitserver klicken Sie auf *Lookup*, um eine SLP-Abfrage für verfügbare Zeitserver in Ihrem Netzwerk zu starten. Wählen Sie den am besten geeigneten Zeitserver in der Liste der Suchergebnisse aus und schließen Sie das Dialogfeld mit *OK*. Bei einem öffentlichen Zeitserver wählen Sie in der Liste unter *Öffentlicher NTP-Server* Ihr Land (Ihre Zeitzone) sowie einen geeigneten Server aus und schließen das Dialogfeld dann mit *OK*. Überprüfen Sie im Hauptdialogfeld die Verfügbarkeit des ausgewählten Servers mit *Test*. Unter *Optionen* können Sie weitere Optionen für `ntpd` einstellen.

  Mit den *Access Control Options* (Zugriffskontrolloptionen) können Sie die Aktionen einschränken, die der entfernte Computer mit dem Daemon Ihres Computers ausführen kann. Dieses Feld ist nur aktiviert, wenn die Option *Restrict NTP Service to Configured Servers Only* (NTP-Dienst auf konfigurierte Server beschränken) auf dem Karteireiter *Sicherheitseinstellungen* aktiviert ist (siehe Abbildung 25.2, „Erweiterte NTP-Konfiguration: Sicherheitseinstellungen" (S. 395)). Die Optionen entsprechen den `restrict`-Klauseln der Datei `/etc/ntp.conf`. Die Klausel

`nomodify notrap noquery` verhindert beispielsweise, dass der Server die NTP-Einstellungen Ihres Computers ändern und die Trap-Funktion (eine Fernprotokollierungsfunktion für Ereignisse) Ihres NTP-Daemons verwenden kann. Diese Einschränkungen werden besonders für Server außerhalb Ihrer Kontrolle empfohlen (z. B. im Internet).

Ziehen Sie bezüglich detaillierter Informationen `/usr/share/doc/packages/ntp-doc` zurate (Bestandteil des `ntp-doc`-Pakets).

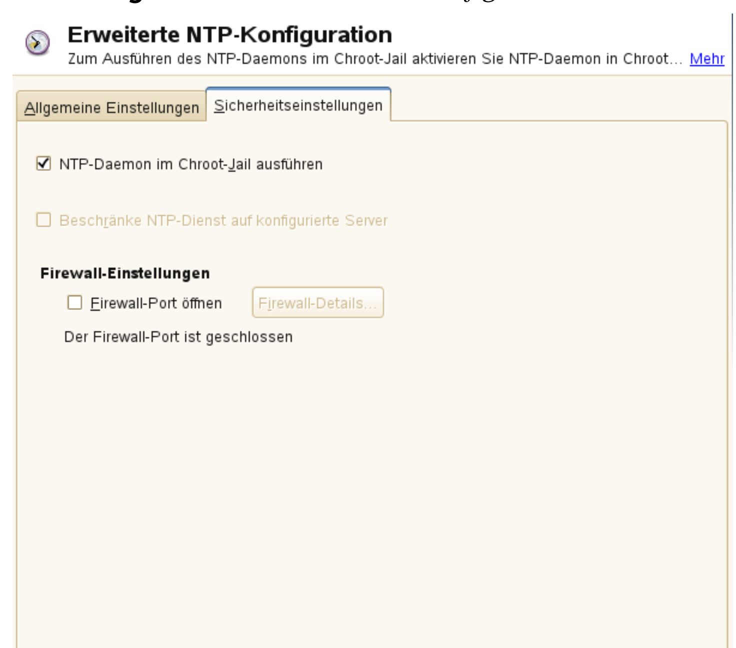
Peer
: Ein Peer ist ein Computer, mit dem eine symmetrische Beziehung eingerichtet wird: Er fungiert sowohl als Zeitserver als auch als Client. Wenn Sie einen Peer im selben Netzwerk anstelle eines Servers verwenden möchten, geben Sie die Adresse des Systems ein. Der Rest des Dialogfelds ist mit dem Dialogfeld *Server* identisch.

Funkuhr
: Wenn eine Funkuhr für die Zeitsynchronisierung in Ihrem System verwendet werden soll, geben Sie Uhrtyp, Gerätezahl, Gerätename und weitere Optionen in diesem Dialogfeld ein. Klicken Sie auf *Treiber-Kalibirierung*, um den Treiber genauer einzustellen. Detaillierte Informationen zum Betrieb einer lokalen Funkuhr finden Sie in `/usr/share/doc/packages/ntp-doc/refclock.html`.

Ausgangs-Broadcast
: Zeitinformationen und Abfragen können im Netzwerk auch per Broadcast übermittelt werden. Geben Sie in diesem Dialogfeld die Adresse ein, an die Broadcasts gesendet werden sollen. Die Option für Broadcasts sollte nur aktiviert werden, wenn Ihnen eine zuverlässige Zeitquelle, etwa eine funkgesteuerte Uhr, zur Verfügung steht.

Eingangs-Broadcast
: Wenn Ihr Client die entsprechenden Informationen per Broadcast erhalten soll, geben Sie in diesen Feldern die Adresse ein, von der die jeweiligen Pakete akzeptiert werden sollen.

Abbildung 25.2 *Erweiterte NTP-Konfiguration: Sicherheitseinstellungen*



Legen Sie auf dem Karteireiter *Sicherheitseinstellungen* (siehe Abbildung 25.2, „Erweiterte NTP-Konfiguration: Sicherheitseinstellungen“ (S. 395)) fest, ob `ntpd` in einem „Chroot Jail“ gestartet werden soll. Standardmäßig ist *DHCP-Daemon in Chroot-Jail starten* aktiviert. Hierdurch wird die Sicherheit im Falle eines Angriffs über `ntpd` erhöht, da der Angreifer daran gehindert wird, das gesamte System zu beeinträchtigen.

Die Option *NTP-Dienst auf konfigurierte Server beschränken* erhöht die Sicherheit Ihres Systems. Wenn gewählt, verhindert diese Option, dass entfernte Computer die NTP-Einstellungen Ihres Computers anzeigen und ändern und die Trap-Funktion für die Fernprotokollierung von Ereignissen verwenden können. Wenn gewählt, gelten diese Einschränkungen für alle entfernten Computer, es sei denn, Sie überschreiben die Zugriffskontrolloptionen für einzelne Computer in der Liste der Zeitquellen auf dem Karteireiter *Allgemeine Einstellungen*. Allen anderen entfernten Computern wird nur die Abfrage der lokalen Zeit erlaubt.

Aktivieren Sie *Firewall-Port öffnen*, wenn SuSEfirewall2 aktiviert ist (Standardeinstellung). Wenn Sie den Port geschlossen lassen, können Sie keine Verbindung zum Zeitserver herstellen.

25.2 Manuelle Konfiguration von NTP im Netzwerk

Die einfachste Art der Verwendung eines Zeitservers im Netzwerk besteht darin, Serverparameter festzulegen. Wenn beispielsweise ein Zeitserver mit der Bezeichnung `ntp.example.com` vom Netzwerk aus erreichbar ist, ergänzen Sie die Datei `/etc/ntp.conf` um seinen Namen, indem Sie die folgende Zeile hinzufügen:

```
server ntp.example.com
```

Wenn Sie weitere Zeitserver hinzufügen möchten, fügen Sie zusätzliche Zeilen mit dem Schlüsselwort `server` ein. Nach der Initialisierung von `ntpd` mit dem Kommando `rcntp start` dauert es etwa eine Stunde, bis die Zeit stabil ist und die Drift-Datei für das Korrigieren der lokalen Computeruhr erstellt wird. Mithilfe der Drift-Datei kann der systematische Fehler der Hardware-Uhr berechnet werden, sobald der Computer eingeschaltet wird. Die Korrektur kommt umgehend zum Einsatz und führt zu einer größeren Stabilität der Systemzeit.

Es gibt zwei Möglichkeiten, den NTP-Mechanismus als Client zu verwenden: Erstens kann der Client in regelmäßigen Abständen die Zeit von einem bekannten Server abfragen. Wenn viele Clients vorhanden sind, kann dies zu einer starken Auslastung des Servers führen. Zweitens kann der Client auf NTP-Broadcasts warten, die von Broadcast-Zeitservern im Netzwerk gesendet werden. Dieser Ansatz hat den Nachteil, dass die Qualität des Servers unbekannt ist und dass ein Server, der falsche Informationen sendet, zu schwerwiegenden Problemen führen kann.

Wenn die Zeit per Broadcast ermittelt wird, ist der Servername nicht erforderlich. Geben Sie in diesem Fall die Zeile `broadcastclient` in die Konfigurationsdatei `/etc/ntp.conf` ein. Wenn ein oder mehrere bekannte Zeitserver exklusiv verwendet werden sollen, geben Sie die Namen in der Zeile ein, die mit `servers` beginnt.

25.3 Dynamische Zeitsynchronisierung während der Laufzeit

Wenn das System ohne Netzwerkverbindung startet, fährt `ntpd` zwar hoch, kann jedoch nicht die DNS-Namen der in der Konfigurationsdatei festgelegten Zeitserver auflösen. Dies kann vorkommen, wenn Sie Network Manager mit einem verschlüsselten WLAN verwenden.

Wenn `ntpd` die DNS-Namen während der Laufzeit auflösen soll, müssen Sie die Option `Dynamisch` festlegen. Wenn das Netzwerk dann einige Zeit nach dem Start aufgebaut wird, überprüft `ntpd` die Namen erneut und kann die Zeitserver zum Abrufen der Zeit erreichen.

Bearbeiten Sie `/etc/ntp.conf` manuell und fügen Sie `Dynamisch` zu einem oder mehreren `Server`einträgen hinzu:

```
server ntp.example.com dynamic
```

Oder verwenden Sie YaST, und gehen Sie folgendermaßen vor:

1 Klicken Sie in YaST auf *Netzwerkdienste* > *NTP-Konfiguration*.

2 Wählen Sie den Server aus, der konfiguriert werden soll. Klicken Sie anschließend auf *Bearbeiten*.

3 Aktivieren Sie das Feld *Optionen* und fügen Sie `Dynamisch` hinzu. Verwenden Sie ein Leerzeichen zum Trennen, falls bereits andere Optionen eingetragen sind.

4 Klicken Sie auf *OK*, um das Dialogfeld für die Bearbeitung zu schließen. Wiederholen Sie den vorherigen Schritt, um alle Server wunschgemäß zu ändern.

5 Klicken Sie abschließend auf *OK*, um die Einstellungen zu speichern.

25.4 Einrichten einer lokalen Referenzuhr

Das Software-Paket `ntpd`enthält Treiber für das Verbinden lokaler Referenzuhren. Eine Liste unterstützter Uhren steht im Paket `ntp-doc` in der Datei `/usr/share/doc/packages/ntp-doc/refclock.html` zur Verfügung. Jeder Treiber ist mit einer Nummer verknüpft. In NTP wird die eigentliche Konfiguration mit Pseudo-IP-Adressen durchgeführt. Die Uhren werden so in die Datei `/etc/ntp.conf` eingegeben, als ob sie im Netzwerk vorhanden wären. Zu diesem Zweck werden Ihnen spezielle IP-Adressen im Format `127.127.`*`t`*`.`*`u`* zugewiesen. Hierbei steht *`t`* für den Uhrentyp und legt fest, welcher Treiber verwendet wird und *`u`* steht für die Einheit (unit), die die verwendete Schnittstelle bestimmt.

Im Regelfall verfügen die einzelnen Treiber über spezielle Parameter, die die Konfigurationsdetails beschreiben. Die Datei `/usr/share/doc/packages/ntp-doc/drivers/driver`*`NN`*`.html` (*`NN`* steht für die Anzahl der Treiber) bietet Informationen zum jeweiligen Uhrentyp. Für die Uhr vom „Typ 8“ (Funkuhr über serielle Schnittstelle) ist ein zusätzlicher Modus erforderlich, der die Uhr genauer angibt. Das Conrad DCF77-Empfängermodul weist beispielsweise Modus 5 auf. Wenn diese Uhr als bevorzugte Referenz verwendet werden soll, geben Sie das Schlüsselwort `prefer` an. Die vollständige `server`-Zeile für ein Conrad DCF77-Empfängermodul sieht folgendermaßen aus:

```
server 127.127.8.0 mode 5 prefer
```

Für andere Uhren gilt dasselbe Schema. Nach der Installation des Pakets `ntp-doc` steht die Dokumentation für ntp im Verzeichnis `/usr/share/doc/packages/ntp-doc` zur Verfügung. Die Datei `/usr/share/doc/packages/ntp-doc/refclock.html` enthält Links zu den Treiberseiten, auf denen die Treiberparameter beschrieben werden.

Verwendung von NetworkManager 26

NetworkManager ist die ideale Lösung für Notebooks und andere portable Computer. Es unterstützt die neuesten Verschlüsselungstypen und Standards für Netzwerkverbindungen, einschließlich Verbindungen zu Netzwerken, die nach 802.1X geschützt sind. 802.1X ist die „anschlussbasierte Netzwerkzugriffssteuerung des IEEE-Standards für lokale und innerstädtische Netzwerke". Wenn Sie viel unterwegs sind und NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen verkabelten und drahtlosen Netzwerken zu verschwenden. NetworkManager kann automatisch eine Verbindung zu bekannten drahtlosen Netzwerken aufbauen oder mehrere Netzwerkverbindungen parallel verwalten – die schnellste Verbindung wird in diesem Fall als Standard verwendet. Darüber hinaus können Sie zwischen verfügbaren Netzwerken manuell wechseln und Ihre Netzwerkverbindung über ein Miniprogramm im Systemabschnitt der Kontrollleiste verwalten.

Anstelle nur einer Verbindung können mehrere Verbindungen gleichzeitig aktiv sein. Dies ermöglicht Ihnen, Ihr Notebook von einem Ethernet zu trennen und drahtlos verbunden zu bleiben.

26.1 Anwendungsbeispiele für den NetworkManager

NetworkManager enthält eine ausgereifte und intuitive Bedienoberfläche, über die Benutzer mühelos zwischen Netzwerkumgebungen wechseln können. In den folgenden Fällen ist der NetworkManager jedoch ungeeignet:

- Ihr Computer stellt Netzwerkdienste für andere Computer in Ihrem Netzwerk bereit (es handelt sich zum Beispiel um einen DHCP- oder DNS-Server)

- Ihr Computer ist ein Xen-Server oder Ihr System ein virtuelles System innerhalb von Xen.

26.2 Aktivieren oder Deaktivieren von NetworkManager

Auf Notebook-Computern ist NetworkManager standardmäßig aktiviert. Es lässt sich jedoch jederzeit im YaST-Modul „Netzwerkeinstellungen“ aktivieren oder deaktivieren.

1 Starten Sie YaST, und gehen Sie zu *Netzwerkgeräte* > *Netzwerkeinstellungen*.

2 Das Dialogfeld *Netzwerkeinstellungen* wird geöffnet. Klicken Sie auf den Karteireiter *Globale Optionen*.

3 Zum Konfigurieren und Verwalten der Netzwerkverbindungen mit NetworkManager gehen Sie wie folgt vor:

  3a Wählen Sie im Feld *Netzwerkeinrichtungsmethode* die Option *Benutzergesteuert mithilfe von NetworkManager*.

  3b Klicken Sie auf *OK*, und schließen Sie YaST.

  3c Konfigurieren Sie die Netzwerkverbindungen mit NetworkManager gemäß den Anweisungen in Abschnitt 26.3, „Konfigurieren von Netzwerkverbindungen“ (S. 401).

4 Zum Deaktivieren von NetworkManager und zum Steuern des Netzwerks auf gewohnte Weise gehen Sie wie folgt vor:

  4a Wählen Sie im Feld *Netzwerkeinrichtungsmethode* die Option *Traditionelle Methode mit ifup*.

  4b Klicken Sie auf *OK*.

4c Richten Sie Ihre Netzwerkkarte mit YaST mithilfe der automatischen Konfiguration durch DHCP oder mithilfe einer statischen IP-Adresse ein. Alternativ konfigurieren Sie Ihr Modem mit YaST:

- Für DFÜ-Verbindungen verwenden Sie *Netzwerkgeräte* > *Modem*.
- Wählen Sie *Netzwerkgeräte* > *ISDN* , um ein internes ISDN-Modem oder ein USB-ISDN-Modem zu konfigurieren.
- Wählen Sie *Netzwerkgeräte* > *DSL*, um ein internes DSL-Modem oder ein USB-DSL-Modem zu konfigurieren.

Eine ausführliche Beschreibung der Netzwerkkonfiguration mit YaST erhalten Sie unter Abschnitt 23.4, „Konfigurieren von Netzwerkverbindungen mit YaST“ (S. 337) und Kapitel 20, *Wireless LAN* (S. 273).

26.3 Konfigurieren von Netzwerkverbindungen

Konfigurieren Sie nach der Aktivierung von NetworkManager in YaST Ihre Netzwerkverbindungen mit den NetworkManager-Frontends, die in KDE und GNOME verfügbar sind. Die Dialogfelder zur Netzwerkkonfiguration sind für beide Frontends sehr ähnlich. Sie zeigen Registerkarten für alle Arten von Netzwerkverbindungen, z. B. verkabelte, drahtlose, mobile Breitband-, DSL- und VPN-Verbindungen. Auf jeder Registerkarte können Sie Verbindungen dieses Typs hinzufügen, bearbeiten oder löschen. Im Dialogfeld für die KDE-Konfiguration sind die entsprechenden Registerkarten nur aktiv, wenn der Verbindungstyp auf Ihrem System verfügbar ist (abhängig von Hardware und Software). Standardmäßig zeigt KNetworkManager auch umfassende Kurzinfos für die verfügbaren Eingabefelder und Optionen auf jeder Registerkarte an.

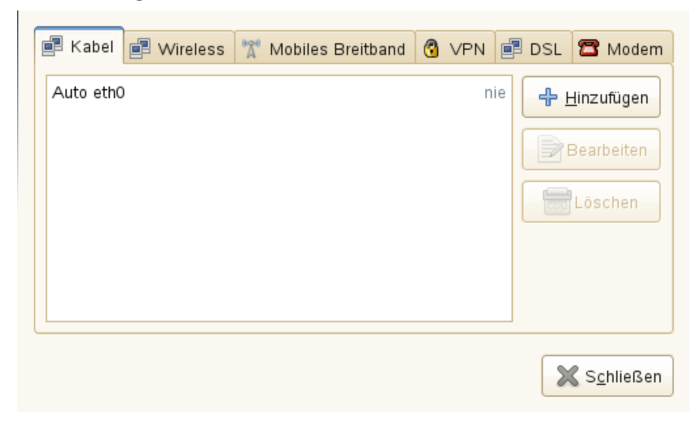
ANMERKUNG: Bluetooth-Verbindungen

Bluetooth-Verbindungen können zur Zeit nicht mit NetworkManager konfiguriert werden.

Öffnen Sie zum Anzeigen des Dialogfelds zur Netzwerkkonfiguration in GNOME das Hauptmenü und klicken Sie rechts auf den Eintrag *Netzwerk*. Drücken Sie alternativ

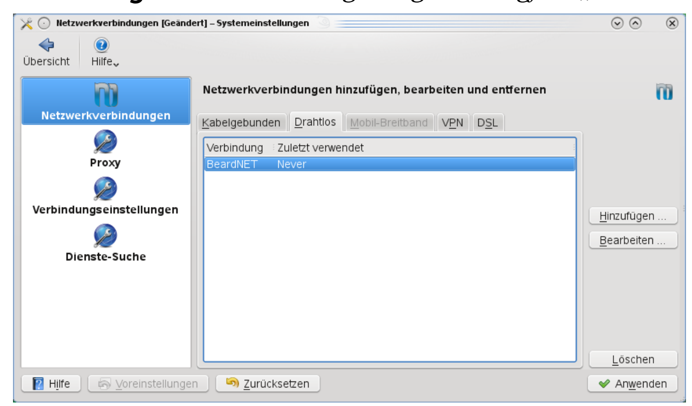
auf Alt + F2 und geben Sie `nm-connection-editor` ein oder wählen Sie im GNOME-Kontrollzentrum *System* > *Netzwerkverbindungen* aus.

Abbildung 26.1 *Dialogfeld „Netzwerkverbindungen“ in GNOME*



Bei Verwendung von KDE öffnen Sie das Hauptmenü und klicken Sie auf *Desktop-Einstellungen*. Wählen Sie auf der Registerkarte *Allgemein* der *Persönlichen Einstellungen* die Option *Netzwerkeinstellungen* aus, um das Dialogfeld zur Netzwerkkonfiguration zu öffnen.

Abbildung 26.2 *KDE-Umgebung – Dialogfeld „Netzwerkkonfiguration“*



Sie können die Konfigurationsdialogfelder alternativ auch aus dem NetworkManager-Miniprogramm im Systemabschnitt der Kontrollleiste starten. Klicken Sie in KDE mit der linken Maustaste auf das Symbol und wählen Sie *Verbindungen verwalten*. Klicken

Sie in GNOME mit der rechten Maustaste auf das Symbol und wählen Sie *Verbindungen bearbeiten*.

ANMERKUNG: Verfügbarkeit von Optionen

Abhängig von Ihrer Systemeinrichtung dürfen Sie möglicherweise keine Verbindungen konfigurieren. In einer abgesicherten Umgebung sind eventuell einige Optionen gesperrt oder verlangen eine `root`-Berechtigung. Erfragen Sie Einzelheiten bei Ihrem Systemadministrator.

Prozedur 26.1 *Hinzufügen oder Bearbeiten von Verbindungen*

Beim Konfigurieren von Netzwerkverbindungen mit NetworkManager können Sie auch `Systemverbindungen` definieren, die für alle Benutzer freigegeben sind. Im Unterschied zu `Benutzerverbindungen` werden Systemverbindungen direkt nach dem Start von NetworkManager und vor der Anmeldung von Benutzern zur Verfügung gestellt. Weitere Einzelheiten über beide Verbindungstypen finden Sie in Abschnitt 26.7.1, „Benutzer- und Systemverbindungen“ (S. 414).

Derzeit steht die Option `Systemverbindung` in KDE nicht zur Verfügung. In diesem Fall müssen Sie zum Einrichten von Systemverbindungen YaST verwenden.

ANMERKUNG: Verborgene Netzwerke

Um eine Verbindung zu einem „verborgenen“ Netzwerk aufzubauen (einem Netzwerk, das seinen Dienst nicht als Broadcast ausführt), müssen Sie den Service Set Identifier (SSID) oder Extended Service Set Identifier (ESSID) des Netzwerks kennen. Verborgene Netzwerke können nicht automatisch gefunden werden.

---

1. Klicken Sie im Dialogfeld für die Netzwerkkonfiguration auf die Registerkarte für den Verbindungstyp, den Sie verwenden möchten.

2. Klicken Sie auf *Hinzufügen*, um eine neue Verbindung zu erstellen, oder wählen Sie eine vorhandene Verbindung aus und klicken Sie auf *Bearbeiten*.

3. Geben Sie einen *Verbindungsnamen* und Ihre Verbindungsdetails ein.

4. Geben Sie für ein verborgenes Netzwerk die ESSID und die Verschlüsselungsparameter ein.

5. Sie können die Verbindung an ein bestimmtes Gerät binden, wenn mehrere physische Geräte pro Verbindungsart verfügbar sind (z. B. wenn Ihr Computer mit zwei Ethernet-Karten oder zwei Wireless-Karten ausgestattet ist).

   Bei Verwendung von KDE erledigen Sie dies über die Option *Restrict to Interface* (Auf Schnittstelle beschränken). Bei Verwendung von GNOME geben Sie die *MAC-Adresse* des Geräts ein, an das Sie die Verbindung binden möchten, und bestätigen Sie Ihre Einstellungen.

6. Damit NetworkManager automatisch eine bestimmte Verbindung nutzt, aktivieren Sie die folgende Option für die gewünschte Verbindung: *Automatisch verbinden* (KDE) oder *Stay connected when possible (Nach Möglichkeit verbunden bleiben)* (GNOME).

7. Zum Umwandeln einer Verbindung in eine `Systemverbindung` aktivieren Sie *Available to all users* (Für alle Benutzer verfügbar) (GNOME). Zum Erstellen und Bearbeiten von Systemverbindungen ist die `root`-Berechtigung erforderlich.

Nachdem Sie Ihre Änderungen bestätigt haben, erscheint die neu konfigurierte Netzwerkverbindung in der Liste der verfügbaren Netzwerke, die Sie erhalten, wenn Sie mit der linken Maustaste auf das NetworkManager-Miniprogramm klicken.

Abbildung 26.3 *KNetworkManager – Konfigurierte und verfügbare Verbindungen*



26.4 Verwenden von KNetworkManager

Das KDE-Frontend für NetworkManager ist die Minianwendung KNetworkManager. Wenn das Netzwerk zur NetworkManager-Steuerung eingerichtet ist, wird das Miniprogramm normalerweise automatisch mit der Desktop-Umgebung gestartet und im Systemabschnitt der Kontrollleiste als Symbol angezeigt.

Wenn im Systemabschnitt der Kontrollleiste kein Symbol für die Netzwerkverbindung angezeigt wird, wurde das Miniprogramm wahrscheinlich nicht gestartet. Drücken Sie Alt + F2 und geben Sie `knetworkmanager` ein, um es manuell zu starten.

KNetworkManager zeigt nur die drahtlosen Netzwerke an, für die Sie eine Verbindung konfiguriert haben. Die Verbindungen werden abgeblendet, wenn Sie nicht mehr in Reichweite eines drahtlosen Netzwerkes sind bzw. wenn das Netzwerkkabel nicht angeschlossen ist. Dadurch behalten Sie immer den Überblick über die Verbindungen, die verwendet werden können.

26.4.1 Verwalten von kabelgebundenen Netzwerkverbindungen

Wenn Ihr Computer mit einem vorhandenen Netzwerk über Netzwerkkabel verbunden ist, wählen Sie die Netzwerkverbindung in KNetworkManager aus.

1. Klicken Sie mit der linken Maustaste auf das Applet-Symbol, um ein Menü mit verfügbaren Netzwerken anzuzeigen. Die aktuell verwendete Verbindung ist im Menü ausgewählt und als *Aktiv* gekennzeichnet.

2. Wenn Sie eine andere Konfiguration mit dem Kabelnetzwerk verwenden möchten, klicken Sie auf *Verbindungen verwalten* und fügen Sie eine andere Kabelverbindung hinzu, wie unter Prozedur 26.1, „Hinzufügen oder Bearbeiten von Verbindungen“ (S. 403) beschrieben.

3. Klicken Sie auf das KNetworkManager-Symbol und wählen Sie die neu konfigurierte Verbindung aus, um sie zu aktivieren.

26.4.2 Verwalten von drahtlosen Netzwerkverbindungen

Standardmäßig zeigt KNetworkManager nur die drahtlosen Netzwerke an, für die Sie eine Verbindung konfiguriert haben, vorausgesetzt, sie sind sowohl verfügbar als auch sichtbar. Gehen Sie folgendermaßen vor, um zum ersten Mal eine Verbindung zu einem drahtlosen Netzwerk herzustellen:

Prozedur 26.2 *Verbinden mit einem drahtlosen Netzwerk*

1. Klicken Sie mit der linken Maustaste auf das Symbol für das Miniprogramm und wählen Sie *Netzwerkverbindung herstellen* aus. KNetworkManager enthält eine Liste der verfügbaren sichtbaren drahtlosen Netzwerke. Diese Liste enthält auch Angaben zur Signalstärke und Sicherheit.

2. Zur Herstellung einer Verbindung zu einem sichtbaren Netzwerk wählen Sie das Netzwerk aus der Liste aus und klicken Sie auf *Verbinden*. Wenn das Netzwerk verschlüsselt ist, öffnet sich ein Dialogfeld. Wählen Sie die Art der *Sicherheit*, die das Netzwerk verwendet, und geben Sie die entsprechenden Berechtigungsnachweise ein.

3. Um eine Verbindung mit einem Netzwerk herzustellen, das seine SSID oder ESSID (Service Set Identifier) nicht sendet und demzufolge nicht automatisch erkannt werden kann, wählen Sie *Connect to Other Network with WLAN interface (Mit anderem Netzwerk über WLAN-Schnittstelle verbinden)*.

4. Geben Sie in dem daraufhin angezeigten Dialogfeld die SSID oder ESSID ein und legen Sie gegebenenfalls die Verschlüsselungsparameter fest.

5. Bestätigen Sie Ihre Änderungen und klicken Sie auf *OK*. NetworkManager aktiviert nun die neue Verbindung.

6. Klicken Sie zum Schließen einer Verbindung und Deaktivierung der drahtlosen Netzwerke auf das Symbol für das Miniprogramm und deaktivieren Sie das Kontrollkästchen für *Drahtlos aktivieren*. Dies kann nützlich sein, wenn Sie sich in einem Flugzeug befinden oder in einer anderen Umgebung, in der drahtlose Netzwerke nicht zulässig sind.

Die Verbindung zu einem drahtlosen Netzwerk, das explizit gewählt wurde, wird so lange wie möglich aufrecht erhalten. Wenn dabei ein Netzwerkkabel angeschlossen ist, werden alle Verbindungen, für die *Automatisch verbinden* festgelegt wurde, hergestellt, während die drahtlose Verbindung bestehen bleibt.

26.4.3 Konfigurieren der drahtlosen Netzwerkkarte als Zugriffspunkt

Wenn Ihre drahtlose Netzwerkkarte den Zugriffspunktmodus unterstützt, können Sie den NetworkManager zur Konfiguration verwenden.

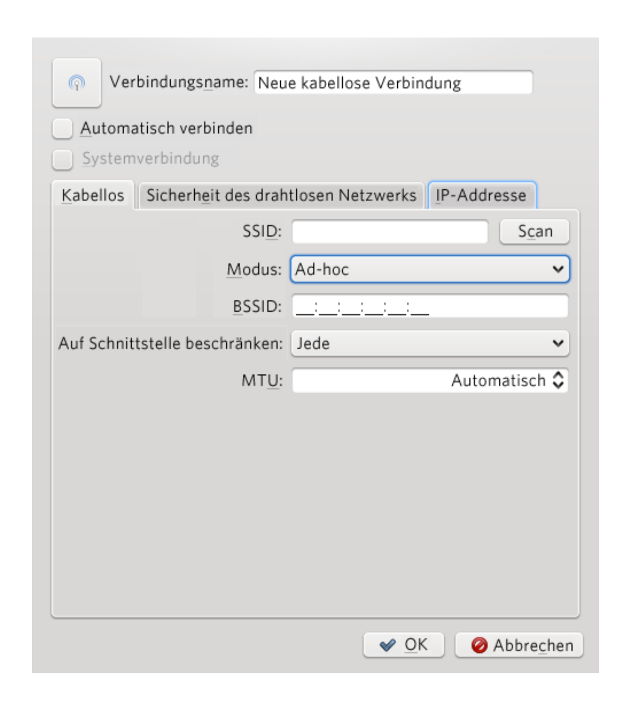
ANMERKUNG: Verfügbarkeit von Optionen

Abhängig von Ihrer Systemeinrichtung dürfen Sie möglicherweise keine Verbindungen konfigurieren. In einer abgesicherten Umgebung sind eventuell einige Optionen gesperrt oder verlangen eine `root`-Berechtigung. Erfragen Sie Einzelheiten bei Ihrem Systemadministrator.

---

1 Klicken Sie auf das KNetworkManager-Miniprogramm und wählen Sie *Netzwerkverbindung herstellen* > *Neues Ad-hoc-Netzwerk*.

2 Geben Sie im folgenden Konfigurationsdialogfeld einen Namen für Ihr Netzwerk im Feld *SSID* ein.



3 Legen Sie die Verschlüsselung im Karteireiter *Drahtlos-Sicherheit* fest.

> **WICHTIG: Ungeschützte drahtlose Netzwerke stellen ein Sicherheitsrisiko dar**
>
> Wenn Sie *Security* (Drahtlose Sicherheit) auf `None` (Keine) einstellen, kann jeder eine Verbindung zu Ihrem Netzwerk herstellen, Ihre Verbindung verwenden und Ihre Netzwerkverbindung abfangen. Verwenden Sie die Verschlüsselung, um den Zugriff auf Ihren Zugriffspunkt zu beschränken und Ihre Verbindung zu schützen. Sie können aus verschiedenen WEP- und WPA-basierten Verschlüsselungen wählen. Wenn Sie sich nicht sicher sind, welche Technologie für Sie am besten geeignet ist, lesen Sie Abschnitt 20.3, „Authentifizierung " (S. 275).

4 Vergewissern Sie sich, dass im Karteireiter *IP-Adresse* die Option *Konfigurieren* auf *Freigegeben* (die Standardoption für Ad-hoc-Netzwerke) festgelegt ist.

5 Bestätigen Sie die Konfiguration mit *OK*.

26.4.4 Anpassen von KNetworkManager

Sie können einige Aspekte von KNetworkManager anpassen: die Anzahl der Symbole, die im Systemabschnitt der Kontrollleiste angezeigt werden, welche Kurztipps angezeigt und wie das Passwort und die Berechtigungsnachweise für die Netzwerkverbindungen gespeichert werden sollen. Weitere Informationen zum letzten Aspekt finden Sie unter Abschnitt 26.7.2, „Speichern von Passwörtern und Berechtigungsnachweisen" (S. 415).

Wenn Sie Informationen zu den verfügbaren Optionen benötigen, klicken Sie mit der rechten Maustaste auf das NetworkManager-Symbol im Systemabschnitt der Kontrollleiste, wählen Sie *Verbindungen verwalten* und klicken Sie auf der linken Seite des Konfigurationsfensters auf *Weitere*.

Prozedur 26.3 *Konfigurieren mehrerer Symbole für KNetworkManager im Systemabschnitt der Kontrollleiste*

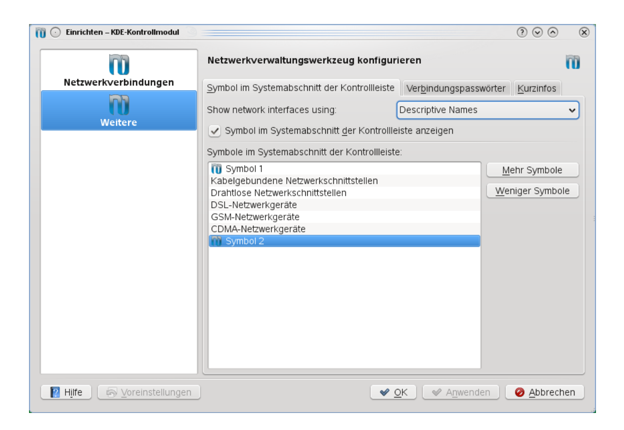
Da in KNetworkManager mehrere Verbindungen gleichzeitig geöffnet sein können, möchten Sie eventuell den Verbindungsstatus der verschiedenen Verbindungen auf einen Blick sehen können. Dies können Sie anhand mehrerer NetworkManager-Symbole im Systemabschnitt der Kontrollleiste erreichen, wobei jedes Symbol eine andere

Gruppe von Verbindungsarten darstellt (zum Beispiel ein Symbol für Kabelverbindungen, ein anderes Symbol für drahtlose Verbindungen).

1 Wechseln Sie im Konfigurationsdialogfeld zum Karteireiter *Symbol für Systemabschnitt der Kontrollleiste*.

2 Klicken Sie auf *Weitere Symbole*. Ein neuer Symboleintrag wird in der Liste angezeigt.

3 Wählen Sie die Arten der Netzwerkverbindungen aus, die durch dieses Symbol dargestellt werden sollen, und gruppieren Sie diese unter dem entsprechenden Symbol.



4 Bestätigen Sie Ihre Änderungen.

Nun werden im Systemabschnitt der Kontrollleiste mehrere NetworkManager-Symbole angezeigt, von denen aus Sie dann auf die mit diesem Symbol verknüpften Verbindungsarten zugreifen können.

Bei der Konfiguration einer Netzwerkverbindung, wie unter Prozedur 26.1, „Hinzufügen oder Bearbeiten von Verbindungen“ (S. 403) beschrieben, ermöglicht Ihnen KNetworkManager auch die Anpassung des für diese Verbindung angezeigten Symbols. Klicken Sie zur Änderung des Symbols auf die Symbolschaltfläche neben *Verbindungsname* und wählen Sie im folgenden Dialogfeld das gewünschte Symbol aus. Nach der Bestätigung Ihrer Änderungen wird das neue Symbol in der Liste der verfügbaren Verbindungen angezeigt, die nach dem Klicken auf das KNetworkManager-Symbol im Systemabschnitt der Kontrollleiste erscheint.

26.5 Verwenden des GNOME NetworkManager-Miniprogramme

In GNOME kann NetworkManager mithilfe des GNOME NetworkManager-Miniprogramms gesteuert werden. Wenn das Netzwerk zur NetworkManager-Steuerung eingerichtet ist, startet das Miniprogramm normalerweise automatisch mit der Desktop-Umgebung und wird im Systemabschnitt der Kontrollleiste als Symbol angezeigt.

Wenn im Systemabschnitt der Kontrollleiste kein Symbol für die Netzwerkverbindung angezeigt wird, wurde das Miniprogramm wahrscheinlich nicht gestartet. Drücken Sie Alt + F2 und geben Sie `nm-applet` ein, um es manuell zu starten.

26.5.1 Verwalten von kabelgebundenen Netzwerkverbindungen

Wenn Ihr Computer mit einem vorhanden Netzwerk über Netzwerkkabel verbunden ist, verwenden Sie das NetworkManager-Miniprogramm zur Auswahl der Netzwerkverbindung.

1. Klicken Sie mit der linken Maustaste auf das Applet-Symbol, um ein Menü mit verfügbaren Netzwerken anzuzeigen. Die zurzeit verwendete Verbindung ist im Menü ausgewählt.

2. Um zu einem anderen Netzwerk zu wechseln, wählen Sie es in der Liste aus.

3. Klicken Sie zum Ausschalten aller Netzwerkverbindungen, sowohl der Kabelverbindungen als auch der drahtlosen Verbindungen, mit der rechten Maustaste auf das Symbol des Miniprogramms und deaktivieren Sie das Kontrollkästchen für *Netzwerk aktivieren*.

26.5.2 Verwalten von drahtlosen Netzwerkverbindungen

Verfügbare sichtbare drahtlose Netzwerke werden im Menü des GNOME NetworkManager-Miniprogramms unter *Drahtlose Netzwerke* aufgeführt. Die Signalstärke der

einzelnen Netzwerke wird ebenfalls im Menü angezeigt. Verschlüsselte drahtlose Netzwerke sind mit einem blauen Schildsymbol gekennzeichnet.

Prozedur 26.4 *Verbinden mit einem drahtlosen Netzwerk*

1. Klicken Sie zum Verbinden mit einem drahtlosen Netzwerk mit der linken Maustaste auf das Symbol für das Miniprogramm und wählen Sie einen Eintrag aus der Liste der verfügbaren drahtlosen Netzwerke aus.

2. Wenn das Netzwerk verschlüsselt ist, öffnet sich ein Dialogfeld. Es gibt den im Netzwerk verwendeten Verschlüsselungstyp an (*Sicherheit des drahtlosen Netzwerks*) und enthält je nach Verschlüsselung und Authentifizierungseinstellung eine Reihe von Eingabefeldern. Geben Sie den korrekten Berechtigungsnachweis ein.

3. Um eine Verbindung mit einem Netzwerk herzustellen, das seine SSID oder ESSID (Service Set Identifier) nicht sendet und demzufolge nicht automatisch erkannt werden kann, klicken Sie mit der linken Maustaste auf das NetworkManager-Symbol, und wählen Sie *Verbindung zu verborgenem drahtlosen Netzwerk herstellen*.

4. Geben Sie im daraufhin angezeigten Dialogfeld unter *Netzwerkname* die SSID oder ESSID ein und legen Sie gegebenenfalls die Verschlüsselungsparameter fest.

5. Um drahtlose Netzwerkverbindungen zu deaktivieren, klicken Sie mit der rechten Maustaste auf das Applet-Symbol und deaktivieren Sie die Option *Drahtlose Netzwerke aktivieren*. Dies kann nützlich sein, wenn Sie sich in einem Flugzeug befinden oder in einer anderen Umgebung, in der drahtlose Netzwerke nicht zulässig sind.

Die Verbindung zu einem drahtlosen Netzwerk, das explizit gewählt wurde, wird so lange wie möglich aufrecht erhalten. Wenn dabei ein Netzwerkkabel angeschlossen ist, werden alle Verbindungen, für die *Stay connected when possible (Nach Möglichkeit verbunden bleiben)* festgelegt wurde, hergestellt, während die drahtlose Verbindung bestehen bleibt.

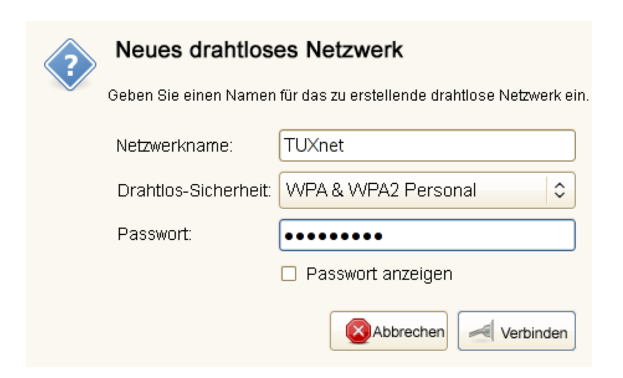
26.5.3 Konfigurieren der drahtlosen Netzwerkkarte als Zugriffspunkt

Wenn Ihre drahtlose Netzwerkkarte den Zugriffspunktmodus unterstützt, können Sie den NetworkManager zur Konfiguration verwenden.

ANMERKUNG: Verfügbarkeit von Optionen

Abhängig von Ihrer Systemeinrichtung dürfen Sie möglicherweise keine Verbindungen konfigurieren. In einer abgesicherten Umgebung sind eventuell einige Optionen gesperrt oder verlangen eine `root`-Berechtigung. Erfragen Sie Einzelheiten bei Ihrem Systemadministrator.

1 Klicken Sie auf das NetworkManager-Miniprogramm, und wählen Sie *Neues drahtloses Netzwerk erstellen*.



2 Geben Sie einen *Netzwerknamen* ein und wählen Sie die gewünschte Verschlüsselung in der Dropdown-Liste *Sicherheit des drahtlosen Netzwerks* aus.

WICHTIG: Ungeschützte drahtlose Netzwerke stellen ein Sicherheitsrisiko dar

Wenn Sie *Wireless Security* (Drahtlose Sicherheit) auf `None` (Keine) einstellen, kann jeder eine Verbindung zu Ihrem Netzwerk herstellen, Ihre Verbindung verwenden und Ihre Netzwerkverbindung abfangen. Verwenden Sie die Verschlüsselung, um den Zugriff auf Ihren Zugriffspunkt zu beschränken und Ihre Verbindung zu schützen. Sie können aus verschiedenen WEP- und WPA-basierten Verschlüsselungen wählen. Wenn Sie sich nicht sicher sind, welche Technologie für Sie am besten geeignet ist, lesen Sie Abschnitt 20.3, „Authentifizierung “ (S. 275).

26.6 NetworkManager und VPN

NetworkManager unterstützt verschiedene Technologien für virtuelle private Netzwerke (VPN). Für jede Technologie bietet SUSE Linux Enterprise Desktop ein Basispaket mit generischer Unterstützung für NetworkManager. Zusätzlich müssen Sie auch das entsprechende Desktop-spezifische Paket für Ihr Miniprogramm installieren.

NovellVPN
: Installieren Sie zur Verwendung dieser VPN-Technik

  - `NetworkManager-novellvpn` und
  - `NetworkManager-novellvpn-kde4` oder `NetworkManager-novellvpn-gnome`.

  NovellVPN-Unterstützung für KDE steht derzeit noch nicht zur Verfügung, es wird jedoch daran gearbeitet.

OpenVPN
: Installieren Sie zur Verwendung dieser VPN-Technik

  - `NetworkManager-openvpn` und
  - `NetworkManager-openvpn-kde4` oder `NetworkManager-openvpn-gnome`.

vpnc (Cisco)
: Installieren Sie zur Verwendung dieser VPN-Technik

  - `NetworkManager-vpnc` und
  - `NetworkManager-vpnc-kde4` oder `NetworkManager-vpnc-gnome`.

PPTP (Point-to-Point-Tunneling-Protokoll)
: Installieren Sie zur Verwendung dieser VPN-Technik

  - `NetworkManager-pptp` und

- `NetworkManager-pptp-kde4` oder `NetworkManager-pptp-gnome`.

Konfigurieren Sie Ihre VPN-Verbindung nach der Installation der Pakete, wie in Abschnitt 26.3, „Konfigurieren von Netzwerkverbindungen“ (S. 401) beschrieben.

26.7 NetworkManager und Sicherheit

Der NetworkManager unterscheidet zwischen zwei Typen von drahtlosen Verbindungen: verbürgte und unverbürgte Verbindungen. Eine verbürgte Verbindung ist jedes Netzwerk, das Sie in der Vergangenheit explizit ausgewählt haben. Alle anderen sind unverbürgt. Verbürgte Verbindungen werden anhand des Namens und der MAC-Adresse des Zugriffspunkts identifiziert. Durch Verwendung der MAC-Adresse wird sichergestellt, dass Sie keinen anderen Zugriffspunkt mit dem Namen Ihrer verbürgten Verbindung verwenden können.

NetworkManager scannt in regelmäßigen Abständen nach verfügbaren drahtlosen Netzwerken. Wenn mehrere verbürgte Netzwerke gefunden werden, wird automatisch das zuletzt verwendete ausgewählt. Wenn keines der Netzwerke vertrauenswürdig ist, wartet NetworkManager auf Ihre Auswahl.

Wenn die Verschlüsselungseinstellung geändert wird, aber Name und MAC-Adresse gleich bleiben, versucht NetworkManager, eine Verbindung herzustellen. Zuvor werden Sie jedoch aufgefordert, die neuen Verschlüsselungseinstellungen zu bestätigen und Aktualisierungen, z. B. einen neuen Schlüssel, bereitzustellen.

Wenn Sie von der Verwendung einer drahtlosen Verbindung in den Offline-Modus wechseln, blendet NetworkManager die SSID oder ESSID aus. So wird sichergestellt, dass die Karte nicht mehr verwendet wird.

26.7.1 Benutzer- und Systemverbindungen

NetworkManager kennt zwei Verbindungsarten: `Benutzer-` und `System-`Verbindungen. Bei Benutzerverbindungen handelt es sich um Verbindungen, die für NetworkManager verfügbar werden, sobald sich der erste Benutzer anmeldet. Alle erforderlichen Legitimationsdaten werden vom Benutzer angefordert, und wenn er sich abmeldet, werden die Verbindungen getrennt und aus NetworkManager entfernt. Als Systemver-

bindung definierte Verbindungen können für alle Benutzer freigegeben werden und sind direkt nach dem Start von NetworkManager verfügbar, bevor sich Benutzer angemeldet haben. Für Systemverbindungen müssen alle Berechtigungsnachweise zum Zeitpunkt der Verbindungserstellung angegeben werden. Über Systemverbindungen können automatisch Verbindungen mit Netzwerken hergestellt werden, für die eine Autorisierung erforderlich ist. Informationen zum Konfigurieren von Benutzer- oder Systemverbindungen mit NetworkManager finden Sie unter Abschnitt 26.3, „Konfigurieren von Netzwerkverbindungen“ (S. 401).

Für KDE wird die Konfiguration von Systemverbindungen mit NetworkManager derzeit nicht unterstützt. (Verwenden Sie stattdessen YaST.)

26.7.2 Speichern von Passwörtern und Berechtigungsnachweisen

Wenn Sie Ihre Berechtigungsnachweise nicht bei jedem Verbindungsversuch mit einem verschlüsselten Netzwerk erneut eingeben möchten, können Sie die Desktop-spezifischen Werkzeuge oder den GNOME Keyring Manager oder KWalletManager verwenden, um Ihre Berechtigungsnachweise verschlüsselt und durch Master-Passwort geschützt auf der Festplatte zu speichern.

In KDE können Sie konfigurieren, ob und wie Ihr Berechtigungsnachweis gespeichert werden soll. Klicken Sie hierfür mit der linken Maustaste auf das NetworkManager-Symbol und wählen Sie *Verbindungen verwalten* aus. Klicken Sie auf *Weitere* > *Verbindungs-Secrets* und wählen Sie eine der folgenden Optionen:

Nicht speichern (Immer auffordern)
: Dies ist nützlich, wenn Sie in einer Umgebung arbeiten, in der das Speichern von Berechtigungsnachweisen als Sicherheitsrisiko betrachtet wird.

In Datei (unverschlüsselt)
: Wenn Sie diese Option wählen, werden Ihre Passwörter unverschlüsselt in der entsprechenden Verbindungsdatei gespeichert, die für jede Verbindung angelegt wird. Diese finden Sie unter `$HOME/.kde4/share/apps/networkmanagement/connections`.

WARNUNG: Sicherheitsrisiko

Das unverschlüsselte Speichern Ihrer Netzwerkberechtigungsnachweise bedeutet ein Sicherheitsrisiko. Jeder, der Zugriff auf Ihren Computer hat, kann Ihre Verbindungsmöglichkeiten nutzen und Ihre Netzwerkverbindung abfangen.

In sicherem Speicher (verschlüsselt)
: Wenn Sie diese Option wählen, werden Ihre Berechtigungsnachweise in KWalletManager gespeichert.Weitere Informationen zu KWalletManager finden Sie unter Chapter 8, *Managing Passwords with KWallet Manager* (↑*KDE User Guide*).

NetworkManager kann auch seine Zertifikate für sichere Verbindungen (z. B. verschlüsselte Kabel-, Funk- oder VPN-Verbindungen) vom Zertifikatspeicher abrufen. Weitere Informationen hierzu finden Sie in Chapter 12, *Certificate Store* (↑*Security Guide*).

26.8 Häufig gestellte Fragen

Nachfolgend finden Sie einige häufig gestellte Fragen zum Konfigurieren spezieller Netzwerkoptionen mit NetworkManager.

Wie kann eine Verbindung an ein bestimmtes Gerät gebunden werden?
: Standardmäßig sind Verbindungen in NetworkManager gerätetypspezifisch: Sie gelten für alle physischen Geräte desselben Typs. Wenn mehrere physische Geräte pro Verbindungsart verfügbar sind (z. B. wenn Ihr Gerät mit zwei Ethernet-Karten ausgestattet ist), können Sie eine Verbindung an ein bestimmtes Gerät binden.

  Schlagen Sie dafür in GNOME zunächst die MAC-Adresse Ihres Geräts in der *Verbindungsinformation* nach, die über das Miniprogramm zur Verfügung steht, oder verwenden Sie die Ausgabe von Kommandozeilenwerkzeugen wie `nm-tool` oder `ifconfig`. Starten Sie dann das Dialogfeld zur Konfiguration von Netzwerkverbindungen und wählen Sie die Verbindung aus, die Sie ändern möchten. Geben Sie auf der Registerkarte *Verkabelt* oder *Drahtlos* die *MAC-Adresse* des Geräts ein und bestätigen Sie Ihre Änderungen.

  Wenn Sie KDE verwenden, starten Sie das Dialogfeld zum Konfigurieren Ihrer Netzwerkverbindungen und wählen Sie die zu ändernde Verbindung aus. Wählen Sie auf der Registerkarte *Ethernet* oder *Drahtlos* mit der Option *Restrict to Interface*

(Auf Schnittstelle beschränken) die Netzwerkschnittstelle aus, an welche die Verbindung gekoppelt werden soll.

Wie wird ein bestimmter Zugriffspunkt angegeben, wenn mehrere Zugriffspunkte mit derselben ESSID erkannt werden?

Wenn mehrere Zugriffspunkte mit unterschiedlichen Funkfrequenzbereichen (a/b/g/n) verfügbar sind, wird standardmäßig der Zugriffspunkt mit dem stärksten Signal automatisch gewählt. Um diesen Vorgang außer Kraft zu setzen, verwenden Sie das Feld *BSSID* beim Konfigurieren Ihrer drahtlosen Verbindungen.

Der Basic Service Set Identifier (BSSID) identifiziert jedes Basic Service Set eindeutig. In einem Basic Service Set der Infrastruktur entspricht die BSSID der MAC-Adresse des drahtlosen Zugriffspunkts. In einem unabhängigen (Ad-hoc) Basic Service Set entspricht die BSSID einer lokal verwalteten MAC-Adresse, die aus einer 46-Bit-Zufallszahl generiert wird.

Starten Sie den Dialog die die Konfiguration von Netzwerkverbindungen wie in Abschnitt 26.3, „Konfigurieren von Netzwerkverbindungen“ (S. 401) beschrieben. Wählen Sie die drahtlose Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Geben Sie im Karteireiter *Drahtlos* die BSSID ein.

Wie werden Netzwerkverbindungen mit anderen Computern freigegeben?

Das primäre Gerät (das Gerät, das mit dem Internet verbunden ist) benötigt keine spezielle Konfiguration. Jedoch müssen Sie das Gerät, das mit dem lokalen Hub oder Computer verbunden ist, wie folgt konfigurieren:

1. Starten Sie den Dialog düe die Konfiguration von Netzwerkverbindungen wie in Abschnitt 26.3, „Konfigurieren von Netzwerkverbindungen“ (S. 401) beschrieben. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Bei Verwendung von GNOME wechseln Sie in die Registerkarte *IPv4-Einstellungen* und wählen Sie aus der Dropdown-Liste *Methode* die Option *Shared to other computers* (Für andere Computer freigegeben). Bei Verwendung von KDE wechseln Sie zum Karteireiter *IP-Adresse* und wählen Sie aus der Dropdown-Liste *Konfigurieren* die Option *Freigegeben*. Damit ist die Weiterleitung von IP-Netzwerkverkehr möglich und ein DHCP-Server wird auf dem Gerät ausgeführt. Bestätigen Sie Ihre Änderungen in NetworkManager.

2. Da der DCHP-Server den Port `67` verwendet, stellen Sie sicher, dass dieser nicht durch die Firewall blockiert ist: Starten Sie YaST auf dem Computer, der die Verbindungen nutzen möchte, und wählen Sie *Sicherheit und Benutzer* > *Firewall*.

Wechseln Sie zur Kategorie *Erlaubte Dienste*. Wenn *DCHP-Server* nicht bereits als *Erlaubter Dienst* angezeigt ist, wählen Sie *DCHP-Server* aus *Services to Allow* (Erlaubte Dienste) und klicken Sie auf *Hinzufügen*. Bestätigen Sie Ihre Änderungen in YaST.

Wie kann statische DNS-Information mit automatischen (DHCP-, PPP-, VPN-) Adressen bereitgestellt werden?

Falls ein DHCP-Server ungültige DNS-Informationen (und/oder Routen) liefert, können Sie diese überschreiben. Starten Sie den Dialog düe die Konfiguration von Netzwerkverbindungen wie in Abschnitt 26.3, „Konfigurieren von Netzwerkverbindungen“ (S. 401) beschrieben. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Bei Verwendung von GNOME öffnen Sie den Karteireiter *IPv4-Einstellungen* und wählen Sie aus der Dropdown-Liste *Methode* die Option *Automatic (DHCP) addresses only* (Nur automatische (DHCP‑) Adressen). Bei Verwendung von KDE öffnen Sie den Karteireiter *IP-Adresse* und wählen Sie aus der Dropdown-Liste *Konfigurieren* die Option *Automatic (DHCP) addresses only* (Nur automatische (DHCP-) Adressen). Geben Sie die DNS-Information in die Felder *DNS-Server* und *Suchdomänen* ein. Sollen automatisch abgerufene Routen ignoriert werden, klicken Sie auf *Routes* (GNOME) und aktivieren Sie das Kontrollkästchen *Ignore automatically obtained routes (Automatisch bezogene Routen ignorieren)* oder wählen Sie in der Dropdown-Liste unten auf dem Karteireiter (KDE) die Option *Routes* und aktivieren Sie das entsprechende Kontrollkästchen. Bestätigen Sie Ihre Änderungen.

Wie kann NetworkManager dazu veranlasst werden, eine Verbindung zu passwortgeschützten Netzwerken aufzubauen, bevor sich ein Benutzer anmeldet?

Definieren Sie eine `Systemverbindung`, die für solche Zwecke verwendet werden kann. Weitere Informationen hierzu finden Sie in Abschnitt 26.7, „NetworkManager und Sicherheit“ (S. 414).

26.9 Fehlersuche

Es können Verbindungsprobleme auftreten. Bei NetworkManager sind unter anderem die Probleme bekannt, dass das Miniprogramm nicht startet oder eine VPN-Option fehlt. Die Methoden zum Lösen und Verhindern dieser Probleme hängen vom verwendeten Werkzeug ab.

NetworkManager-Desktop-Applet wird nicht gestartet
: Die Miniprogramme von GNOME- und KDE NetworkManager starten automatisch, wenn das Netzwerk für die NetworkManager-Steuerung eingerichtet ist. Wenn das Miniprogramm/Widget nicht gestartet wird, überprüfen Sie, ob NetworkManager in YaST aktiviert ist (siehe Abschnitt 26.2, „Aktivieren oder Deaktivieren von NetworkManager" (S. 400)). Vergewissern Sie sich danach, ob das richtige Paket für Ihre Desktop-Umgebung installiert ist. Wenn Sie mit KDE 4 arbeiten, trägt das Paket die Bezeichnung `NetworkManager-kde4`. Wenn Sie mit GNOME arbeiten, trägt das Paket die Bezeichnung `NetworkManager-gnome`.

  Wenn das Desktop-Miniprogramm installiert ist, aber aus einem unbestimmten Grund nicht ausgeführt wird, starten Sie es manuell. Wenn das Desktop-Miniprogramm installiert ist, aber nicht ausgeführt wird, starten Sie es manuell über das Kommando `nm-applet` (GNOME) bzw. `knetworkmanager` (KDE).

Das NetworkManager-Applet beinhaltet keine VPN-Option
: Die Unterstützung für NetworkManager-Miniprogramme sowie VPN für NetworkManager wird in Form separater Pakete verteilt. Wenn Ihr NetworkManager-Applet keine VPN-Option enthält, überprüfen Sie, ob die Pakete mit der NetworkManager-Unterstützung für Ihre VPN-Technologie installiert sind. Weitere Informationen finden Sie unter Abschnitt 26.6, „NetworkManager und VPN" (S. 413).

Keine Netzwerkverbindung verfügbar
: Wenn Sie Ihre Netzwerkverbindung korrekt konfiguriert haben und alle anderen Komponenten für die Netzwerkverbindung (Router etc.) auch gestartet sind und ausgeführt werden, ist es manchmal hilfreich, die Netzwerkschnittstellen auf Ihrem Computer erneut zu starten. Melden Sie sich dazu bei einer Kommandozeile als `root` an, und führen Sie das Kommando `rcnetwork restart` aus.

26.10 Weiterführende Informationen

Weitere Informationen zu NetworkManager finden Sie auf den folgenden Websites und in folgenden Verzeichnissen:

Projektseite von NetworkManager
: http://projects.gnome.org/NetworkManager/

KDE NetworkManager-Frontend
: `http://userbase.kde.org/NetworkManagement`

Dokumentation zu den einzelnen Paketen
: Lesen Sie auch die neuesten Informationen zu NetworkManager und den Miniprogrammen GNOME und KDE NetworkManager in den folgenden Verzeichnissen:

  - `/usr/share/doc/packages/NetworkManager/`,
  - `/usr/share/doc/packages/NetworkManager-kde4/` und
  - `/usr/share/doc/packages/NetworkManager-gnome/`.

27 Samba

Mit Samba kann ein Unix-Computer als Datei- und Druckserver für Mac OS X-, Windows- und OS/2-Computer konfiguriert werden. Samba ist mittlerweile ein sehr umfassendes und komplexes Produkt. Konfigurieren Sie Samba mit YaST, SWAT (eine Web-Schnittstelle) oder indem Sie die Konfigurationsdatei manuell bearbeiten.

27.1 Terminologie

Im Folgenden werden einige Begriffe erläutert, die in der Samba-Dokumentation und im YaST-Modul verwendet werden.

SMB-Protokoll
: Samba verwendet das SMB-Protokoll (Server Message Block), das auf den NetBIOS-Diensten basiert. Microsoft veröffentlichte das Protokoll, damit auch andere Softwarehersteller Anbindungen an ein Microsoft-Domänennetzwerk einrichten konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das TCP/IP-Protokoll installiert sein.

CIFS-Protokoll
: Das CIFS-Protokoll (Common Internet File System) ist ein weiteres von Samba unterstütztes Protokoll. CIFS definiert ein Standardprotokoll für den Fernzugriff auf Dateisysteme über das Netzwerk, das Benutzergruppen die netzwerkweite Zusammenarbeit und gemeinsame Dokumentbenutzung ermöglicht.

NetBIOS
: NetBIOS ist eine Softwareschnittstelle (API) für die Kommunikation zwischen Computern, die einen Name Service bereitstellen. Mit diesem Dienst können die an das Netzwerk angeschlossenen Computer Namen für sich reservieren. Nach dieser Reservierung können die Computer anhand ihrer Namen adressiert werden. Für die Überprüfung der Namen gibt es keine zentrale Instanz. Jeder Computer im Netzwerk kann beliebig viele Namen reservieren, solange die Namen noch nicht Gebrauch sind. Die NetBIOS-Schnittstelle kann in unterschiedlichen Netzwerkarchitekturen implementiert werden. Eine Implementierung, die relativ eng mit der Netzwerkhardware arbeitet, ist NetBEUI (häufig auch als NetBIOS bezeichnet). Mit NetBIOS implementierte Netzwerkprotokolle sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

  Die per TCP/IP übermittelten NetBIOS-Namen haben nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun. NetBIOS ist ein eigener, vollständig unabhängiger Namensraum. Es empfiehlt sich jedoch, für eine einfachere Administration NetBIOS-Namen zu vergeben, die den jeweiligen DNS-Hostnamen entsprechen, oder DNS nativ zu verwenden. Für einen Samba-Server ist dies die Voreinstellung.

Samba-Server
: Samba-Server stellt SMB/CIFS-Dienste sowie NetBIOS over IP-Namensdienste für Clients zur Verfügung. Für Linux gibt es drei Dämonen für Samba-Server: smbd für SMB/CIFS-Dienste, nmbd für Naming Services und winbind für Authentifizierung.

Samba-Client
: Der Samba-Client ist ein System, das Samba-Dienste von einem Samba-Server über das SMB-Protokoll nutzt. Das Samba-Protokoll wird von allen gängigen Betriebssystemen wie Mac OS X, Windows und OS/2 unterstützt. Auf den Computern muss das TCP/IP-Protokoll installiert sein. Für die verschiedenen UNIX-Versionen stellt Samba einen Client zur Verfügung. Für Linux gibt es zudem ein Dateisystem-Kernel-Modul für SMB, das die Integration von SMB-Ressourcen auf Linux-Systemebene ermöglicht. Sie brauchen für den Samba-Client keinen Dämon auszuführen.

Freigaben
: SMB-Server stellen den Clients Ressourcen in Form von Freigaben (Shares) zur Verfügung. Freigaben sind Drucker und Verzeichnisse mit ihren Unterverzeichnissen auf dem Server. Eine Freigabe wird unter einem eigenen Namen exportiert und

kann von Clients unter diesem Namen angesprochen werden. Der Freigabename kann frei vergeben werden. Er muss nicht dem Namen des exportierten Verzeichnisses entsprechen. Ebenso wird einem Drucker ein Name zugeordnet. Clients können mit diesem Namen auf den Drucker zugreifen.

DC
: Ein Domain Controller (DC) ist ein Server, der Konten in der Domäne verwaltet. Zur Datenreplikation stehen zusätzliche Domain Controller in einer Domäne zur Verfügung.

27.2 Konfigurieren eines Samba-Servers

Informationen zum Konfigurieren eines Samba-Servers finden Sie in der Dokumentationen für SUSE Linux Enterprise Server.

27.3 Konfigurieren der Clients

Clients können auf den Samba-Server nur über TCP/IP zugreifen. NetBEUI oder NetBIOS über IPX können mit Samba nicht verwendet werden.

27.3.1 Konfigurieren eines Samba-Clients mit YaST

Konfigurieren Sie einen Samba-Client, um auf Ressourcen (Dateien oder Drucker) auf dem Samba- oder Windows-Server zuzugreifen. Geben Sie im Dialogfeld *Netzwerkdienste* > *Windows-Domänenmitgliedschaft* die NT- oder Active Directory-Domäne oder -Arbeitsgruppe an. Wenn Sie *Zusätzlich SMB-Informationen für Linux-Authentifizierung verwenden* aktivieren, erfolgt die Benutzerauthentifizierung über den Samba‑, NT- oder Kerberos-Server.

Klicken Sie für erweiterte Konfigurationsoptionen auf *Einstellungen für Experten*. Sie können z. B. über die Tabelle *Serververzeichnisse einhängen* das automatische Einhängen des Server-Basisverzeichnisses bei der Authentifizierung aktivieren. Auf diese

Weise können Benutzer auf ihre Home-Verzeichnisse zugreifen, wenn diese in CIFS gehostet sind. Einzelheiten finden Sie auf der man-Seite `pam_mount`.

Bestätigen Sie zum Abschluss alle Einstellungen, um die Konfiguration zu beenden.

27.4 Samba als Anmeldeserver

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich Benutzer nur mit einem gültigen Konto und zugehörigem Passwort anmelden dürfen. In einem Windows-basierten Netzwerk wird diese Aufgabe von einem Primary Domain Controller (PDC) übernommen. Sie können einen Windows NT-Server verwenden, der als PDC konfiguriert ist; diese Aufgabe kann aber auch mithilfe eines Samba-Servers ausgeführt werden. Es müssen Einträge im Abschnitt `[global]` von `smb.conf` vorgenommen werden. Diese werden in Beispiel 27.1, „Abschnitt „global“ in smb.conf“ (S. 424) beschrieben.

Beispiel 27.1 *Abschnitt „global“ in smb.conf*

```
[global]
    workgroup = TUX-NET
    domain logons = Yes
    domain master = Yes
```

Wenn verschlüsselte Passwörter zur Verifizierung verwendet werden, muss der Samba-Server in der Lage sein, diese zu verwalten. Dies wird durch den Eintrag `encrypt passwords = yes` im Abschnitt `[global]` aktiviert (ab Samba Version 3 ist dies Standard). Außerdem müssen die Benutzerkonten bzw. die Passwörter in eine Windows-konforme Verschlüsselungsform gebracht werden. Dies erfolgt mit dem Befehl `smbpasswd-a name`. Da nach dem Windows-Domänenkonzept auch die Computer selbst ein Domänenkonto benötigen, wird dieses mit den folgenden Kommandos angelegt:

```
useradd hostname\$
smbpasswd -a -m hostname
```

Mit dem Befehl `useradd` wird ein Dollarzeichen hinzugefügt. Der Befehl `smbpasswd` fügt dieses bei der Verwendung des Parameters `-m` automatisch hinzu. In der kommentierten Beispielkonfiguration (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) sind Einstellungen enthalten, die diese Aufgabe automatisieren.

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Um sicherzustellen, dass Samba dieses Skript korrekt ausführen kann, wählen Sie einen Samba-Benutzer mit den erforderlichen Administratorberechtigungen und fügen Sie ihn zur Gruppe `ntadmin` hinzu. Anschließend können Sie allen Mitgliedern der Linux-Gruppe den Status `Domain Admin` zuweisen, indem Sie folgendes Kommando eingeben:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Weitere Informationen zu diesem Thema finden Sie in Kapitel 12 in Samba 3 HOWTO (`/usr/share/doc/packages/samba/Samba3-HOWTO.pdf`).

27.5 Weiterführende Informationen

Ausführliche Informationen zu Samba finden Sie in der digitalen Dokumentation. Wenn Samba installiert ist, können Sie in der Kommandozeile `apropos samba` eingeben, um einige man-Seiten aufzurufen. Alternativ dazu finden Sie im Verzeichnis `/usr/share/doc/packages/samba` weitere Online-Dokumentationen und Beispiele. Eine kommentierte Beispielkonfiguration (`smb.conf.SuSE`) finden Sie im Unterverzeichnis `examples`.

Das Samba-Team liefert in Samba 3 HOWTO einen Abschnitt zur Fehlerbehebung. In Teil V ist außerdem eine ausführliche Anleitung zum Überprüfen der Konfiguration enthalten. Nach der Installation des Pakets `samba-doc` finden Sie das Samba 3 HOWTO-Dokument im Verzeichnis
`/usr/share/doc/packages/samba/Samba3-HOWTO.pdf`.



Verteilte Nutzung von Dateisystemen mit NFS 28

Das Verteilen und Freigeben von Dateisystemen über ein Netzwerk ist eine Standardaufgabe in Unternehmensumgebungen. Das bewährte Netzwerkdateisystem *NFS* arbeitet mit dem Verzeichnisdienst *NIS* zusammen. Wenn Sie ein sichereres Protokoll wünschen, das mit *LDAP* zusammenarbeitet und auch Kerberos nutzen kann, aktivieren Sie *NFSv4*. Zusammen mit pNFS können Sie so Engpässe bei der Leistung beseitigen.

NFS mit NIS macht ein Netzwerk für den Benutzer transparent. Mit NFS ist es möglich, arbiträre Dateisysteme über das Netzwerk zu verteilen. Bei entsprechendem Setup befinden sich Benutzer in derselben Umgebung, unabhängig vom gegenwärtig verwendeten Terminal.

28.1 Terminologie

Die folgenden Begriffe werden im YaST-Modul verwendet.

Exporte
: Ein von einem NFS-Server *exportiertes* Verzeichnis, das von Clients in ihr System integriert werden kann.

NFS-Client
: Der NFS-Client ist ein System, das NFS-Dienste eines NFS-Servers über das NFS-Protokoll verwendet. Das TCP/IP-Protokoll ist bereits in den Linux-Kernel integriert, weshalb keine zusätzliche Software installiert werden muss.

NFS-Server
: Der NFS-Server stellt NFS-Dienste für Clients bereit. Die Ausführung eines Servers hängt von folgenden Daemons ab: `nfsd` (Worker), `idmapd` (Zuordnung von Benutzer- und Gruppennamen zu IDs und umgekehrt), `statd` (Dateisperrung) und `mountd` (Einhängen-Anforderungen).

pNFS
: Parallel NFS, eine Protokollerweiterung für NFSv4. Alle pNFS-Clients können direkt auf die Daten auf einem NFS-Server zugreifen.

28.2 Installieren des NFS-Servers

Die NFS-Server-Software ist kein Bestandteil der Standardinstallation. Wenn Sie einen NFS-Server gemäß den Anweisungen unter Abschnitt 28.3, „Konfigurieren des NFS-Servers“ (S. 428) konfigurieren, werden Sie automatisch aufgefordert, die erforderlichen Pakete zu installieren. Alternativ installieren Sie das Paket `nfs-kernel-server` mit YaST oder Zypper.

Wie NIS ist NFS ein Client-Server-System. Ein Rechner kann jedoch beides gleichzeitig sein – er kann Dateisysteme im Netzwerk zur Verfügung stellen (exportieren) und Dateisysteme anderer Hosts mounten (importieren).

28.3 Konfigurieren des NFS-Servers

Die Konfiguration eines NFS-Servers kann über YaST oder manuell erfolgen. NFS kann für die Authentifizierung auch mit Kerberos kombiniert werden.

28.3.1 NFS mit Kerberos

Wenn die Kerberos-Authentifizierung für NFS verwendet werden soll, muss die GSS-Sicherheit aktiviert werden. Wählen Sie im ersten YaST-NFS-Server-Dialogfeld die Option *GSS-Sicherheit aktivieren*. Zur Verwendung dieser Funktion muss ein funktionierender Kerberos-Server zur Verfügung stehen. YaST richtet diesen Server nicht ein, sondern nutzt lediglich die über den Server bereitgestellten Funktionen. Wenn Sie die Authentifizierung mittels Kerberos verwenden möchten, müssen Sie zusätzlich zur

YaST-Konfiguration mindestens die nachfolgend beschriebenen Schritte ausführen, bevor Sie die NFS-Konfiguration ausführen:

1 Stellen Sie sicher, dass sich Server und Client in derselben Kerberos-Domäne befinden. Beide müssen auf denselben KDC-Server (Key Distribution Center) zugreifen und die Datei `krb5.keytab` gemeinsam verwenden (der Standardspeicherort auf allen Rechnern lautet `/etc/krb5.keytab`). Weitere Informationen zu Kerberos finden Sie unter Chapter 6, *Network Authentication with Kerberos* (↑*Security Guide*).

2 Starten Sie den gssd-Dienst auf dem Client mit `rcgssd start`.

Weitere Informationen zum Konfigurieren eines kerberisierten NFS finden Sie über die Links in Abschnitt 28.5, „Weiterführende Informationen“ (S. 433).

28.4 Konfigurieren der Clients

Wenn Sie Ihren Host als NFS-Client konfigurieren möchten, müssen Sie keine zusätzliche Software installieren. Alle erforderlichen Pakete werden standardmäßig installiert.

28.4.1 Importieren von Dateisystemen mit YaST

Autorisierte Benutzer können NFS-Verzeichnisse eines NFS-Servers über das YaST-NFS-Clientmodul in den lokalen Dateibaum einhängen. Führen Sie dazu die folgenden Schritte aus:

Prozedur 28.1 *Importieren von NFS-Verzeichnissen*

1 Starten Sie das YaST-NFS-Client-Modul.

2 Klicken Sie auf dem Karteireiter *NFS-Freigaben* auf *Hinzufügen*. Geben Sie den Hostnamen des NFS-Servers, das zu importierende Verzeichnis und den Einhängepunkt an, an dem das Verzeichnis lokal eingehängt werden soll.

3 Wenn Sie eine Firewall nutzen und den Zugriff auf den Dienst von Ferncomputern aus zulassen möchten, aktivieren Sie auf dem Karteireiter *NFS-Einstellungen* die

Option *Firewall-Port öffnen*. Der Status der Firewall wird neben dem Kontrollkästchen angezeigt.

4 Wenn Sie NFSv4 verwenden, vergewissern Sie sich, dass das Kontrollkästchen für *NFSv4 aktivieren* aktiviert ist und dass der *NFSv4-Domänenname* denselben Wert enthält, den der NFSv4-Server verwendet. Die Standarddomäne ist `localdomain`.

5 Klicken Sie zum Speichern der Änderungen auf *OK*.

Die Konfiguration wird in `/etc/fstab` geschrieben und die angegebenen Dateisysteme werden eingehängt. Wenn Sie den YaST-Konfigurationsclient zu einem späteren Zeitpunkt starten, wird auch die vorhandene Konfiguration aus dieser Datei gelesen.

28.4.2 Manuelles Importieren von Dateisystemen

Voraussetzung für den manuellen Import eines Dateisystems von einem NFS-Server ist ein aktiver RPC-Port-Mapper. Diesen starten Sie durch Ausführung von `rcrpcbind start` als `Root`. Danach können ferne Dateisysteme mit `mount` wie lokale Partitionen in das Dateisystem eingehängt werden:

```
mount host:remote-pathlocal-path
```

Geben Sie zum Beispiel zum Import von Benutzerverzeichnissen vom `nfs.example.com`-Rechner folgendes Kommando ein:

```
mount nfs.example.com:/home /home
```

28.4.2.1 Verwenden des Diensts zum automatischen Einhängen

Ferne Dateisysteme können mit dem autofs-Daemon automatisch eingehängt werden. Fügen Sie den folgenden Eintrag in der Datei `/etc/auto.master` hinzu:

```
/nfsmounts /etc/auto.nfs
```

Nun fungiert das Verzeichnis `/nfsmounts` als Root-Verzeichnis für alle NFS-Einhängungen auf dem Client, sofern die Datei `auto.nfs` entsprechend ausgefüllt wurde. Der Name `auto.nfs` wurde nur der Einfachheit halber ausgewählt – Sie können einen

beliebigen Namen auswählen. Fügen Sie der Datei `auto.nfs` wie folgt Einträge für alle NFS-Einhängungen hinzu:

```
localdata -fstype=nfs server1:/data
nfs4mount -fstype=nfs4 server2:/
```

Aktivieren Sie die Einstellungen durch Ausführung von `rcautofs start` als `root`. In diesem Beispiel wird `/nfsmounts/localdata`, das Verzeichnis `/data` von `server1`, mit NFS eingehängt und `/nfsmounts/nfs4mount` von `server2` wird mit NFSv4 eingehängt.

Wenn die Datei `/etc/auto.master` während der Ausführung des Diensts autofs bearbeitet wird, muss die automatische Einhängung mit `rcautofs restart` erneut gestartet werden, damit die Änderungen wirksam werden.

28.4.2.2 Manuelles Bearbeiten von /ect/fstab

Ein typischer NFSv3-Einhängeeintrag in `/etc/fstab` sieht folgendermaßen aus:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

Auch NFSv4-Einhängungen können der Datei `/etc/fstab` hinzugefügt werden. Verwenden Sie für diese Einhängungen in der dritten Spalte `nfs4` statt `nfs` und stellen Sie sicher, dass das entfernte Dateisystem in der ersten Spalte nach *`nfs.example.com:`* als `/` angegeben ist. Eine typische Zeile für eine NFSv4-Einhängung in `/etc/fstab` sieht zum Beipsiel wie folgt aus:

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

Mit der Option `noauto` wird verhindert, dass das Dateisystem beim Starten automatisch eingehängt wird. Wenn Sie das jeweilige Dateisystem manuell einhängen möchten, können Sie das Einhängekommando auch kürzen, indem Sie nur den Einhängepunkt angeben:

```
mount /local/path
```

Beachten Sie, dass das Einhängen dieser Dateisysteme beim Start durch die Initialisierungsskripte des Systems geregelt wird, wenn die Option `noauto` nicht angegeben ist.

28.4.3 pNFS (paralleles NFS)

NFS wurde in den 1980er-Jahren entwickelt und gehört damit zu den ältesten Protokollen. Zum Freigeben kleinerer Dateien ist NFS völlig ausreichend. Wenn Sie dagegen große Dateien übertragen möchten oder wenn zahlreiche Clients auf die Daten zugreifen sollen, wird ein NFS-Server rasch zu einer Engstelle, die die Systemleistungen erheblich beeinträchtigt. Dies liegt daran, dass die Dateien rasch größer werden, wobei die relative Ethernet-Geschwindigkeit nicht ganz mithalten kann.

Wenn Sie eine Datei von einem „normalen" NFS-Server anfordern, werden die Metadaten der Datei nachgeschlagen, die Daten dieser Datei werden zusammengestellt und die Datei wird schließlich über das Netzwerk an den Client übertragen. Der Leistungsengpass wird jedoch in jedem Fall ersichtlich, unabhängig davon, wie groß oder klein die Dateien sind:

- Bei kleinen Dateien dauert das Sammeln der Metadaten am längsten.
- Bei großen Dateien dauert das Übertragen der Daten vom Server auf den Client am längsten.

pNFS (paralleles NFS) trennt die Metadaten des Dateisystems vom Speicherort der Daten und überwindet so diese Einschränkungen. Für pNFS sind dabei zwei Arten von Servern erforderlich:

- Ein *Metadaten-* oder *Steuerungsserver*, der den gesamten verbleibenden Verkehr (nicht den Datenverkehr) abwickelt
- Mindestens ein *Speicherserver*, auf dem sich die Daten befinden

Der Metadatenserver und die Speicherserver bilden gemeinsam einen einzigen logischen NFS-Server. Wenn ein Client einen Lese- oder Schreibvorgang startet, teilt der Metadatenserver dem NFSv4-Client mit, auf welchem Speicherserver der Client auf die Dateiblöcke zugreifen soll. Der Client kann direkt auf dem Server auf die Daten zugreifen.

SUSE Linux Enterprise unterstützt pNFS nur auf der Clientseite.

28.4.3.1 Konfigurieren eines pNTP-Clients mit YaST

Befolgen Sie die Anweisungen unter Prozedur 28.1, „Importieren von NFS-Verzeichnissen“ (S. 429); aktivieren Sie jedoch das Kontrollkästchen *pNFS (v4.1)* und (optional) *NFSv4-Freigabe*. YaST führt alle erforderlichen Schritte aus und schreibt die erforderlichen Optionen in die Datei `/etc/exports`.

28.4.3.2 Manuelles Konfigurieren eines pNTP-Clients

Beginnen Sie gemäß Abschnitt 28.4.2, „Manuelles Importieren von Dateisystemen“ (S. 430). Der Großteil der Konfiguration wird durch den NFSv4-Server ausgeführt. Der einzige Unterschied für pNFS besteht darin, dass die Option `minorversion` und der Metadatenserver *`MDS_SERVER`* in das Kommando `mount` eingefügt werden:

```
mount -t nfs4 -o minorversion=1 MDS_SERVER MOUNTPOINT
```

Als Hilfe für die Fehlersuche ändern Sie den Wert im Dateisystem `/proc`:

```
echo 32767 > /proc/sys/sunrpc/nfsd_debug
echo 32767 > /proc/sys/sunrpc/nfs_debug
```

28.5 Weiterführende Informationen

Außer auf den man-Seiten zu `exports`, `nfs` und `mount` stehen Informationen zum Konfigurieren eines NFS-Servers und -Clients unter `/usr/share/doc/packages/nfsidmap/README` zur Verfügung. Weitere Online-Dokumentation finden Sie auf folgenden Websites:

- Die detaillierte technische Dokumentation finden Sie online unter SourceForge [http://nfs.sourceforge.net/].
- Anweisungen zum Einrichten eines kerberisierten NFS finden Sie unter NFS Version 4 Open Source Reference Implementation [http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html].
- Falls Sie Fragen zu NFSv4 haben, lesen Sie die Linux NFSv4-FAQ [http://www.citi.umich.edu/projects/nfsv4/linux/faq/].



29 Dateisynchronisierung

Viele Menschen benutzen heutzutage mehrere Computer: einen Computer zu Hause, einen oder mehrere Computer am Arbeitsplatz und eventuell ein Notebook, ein Tablet oder ein Smartphone unterwegs. Viele Dateien werden auf allen diesen Computern benötigt. Vermutlich wollen Sie Ihre Dateien auf allen Computern bearbeiten und benötigen die Daten daher auf allen Computern auf dem aktuellsten Stand.

29.1 Verfügbare Software zur Datensynchronisierung

Auf Computern, die ständig miteinander über ein schnelles Netzwerk in Verbindung stehen, ist die Datensynchronisierung kein Problem. In diesem Fall wählen Sie ein Netzwerkdateisystem, wie zum Beispiel NFS, und speichern die Dateien auf einem Server. Alle Rechner greifen dabei über das Netzwerk auf ein und dieselben Daten zu. Dieser Ansatz ist unmöglich, wenn die Netzverbindung schlecht oder teilweise gar nicht vorhanden ist. Wer mit einem Laptop unterwegs ist, ist darauf angewiesen, von allen benötigten Dateien Kopien auf der lokalen Festplatte zu haben. Wenn Dateien bearbeitet werden, stellt sich aber schnell das Problem der Synchronisierung. Wenn Sie eine Datei auf einem Computer ändern, stellen Sie sicher, dass die Kopie der Datei auf allen anderen Computern aktualisiert wird. Dies kann bei gelegentlichen Kopiervorgängen manuell mithilfe von scp oder rsync erledigt werden. Bei vielen Dateien wird das jedoch schnell aufwändig und erfordert hohe Aufmerksamkeit vom Benutzer, um Fehler, wie etwa das Überschreiben einer neuen mit einer alten Datei, zu vermeiden.

WARNUNG: Risiko des Datenverlusts

Bevor Sie Ihre Daten mit einem Synchronisierungssystem verwalten, sollten Sie mit dem verwendeten Programm vertraut sein und dessen Funktionalität testen. Für wichtige Dateien ist das Anlegen einer Sicherungskopie unerlässlich.

Zur Vermeidung der zeitraubenden und fehlerträchtigen manuellen Arbeit bei der Datensynchronisierung gibt es Programme, die diese Aufgabe mit verschiedenen Ansätzen automatisieren. Die folgenden Zusammenfassungen sollen dem Benutzer eine Vorstellung davon liefern, wie diese Programme funktionieren und genutzt werden können. Vor dem tatsächlichen Einsatz sollten Sie die Programmdokumentation sorgfältig lesen.

29.1.1 CVS

CVS, das meistens zur Versionsverwaltung von Quelltexten von Programmen benutzt wird, bietet die Möglichkeit, Kopien der Dateien auf mehreren Computern zu führen. Damit eignet es sich auch für die Datensynchronisierung. CVS führt ein zentrales Repository auf dem Server, das nicht nur die Dateien, sondern auch die Änderungen an ihnen speichert. Lokal erfolgte Änderungen werden an das Repository übermittelt und können von anderen Computern durch ein Update abgerufen werden. Beide Prozeduren müssen vom Benutzer initiiert werden.

Dabei ist CVS bei gleichzeitigen Änderungen einer Datei auf mehreren Computern sehr fehlertolerant. Die Änderungen werden zusammengeführt, und falls in gleichen Zeilen Änderungen vorgenommen wurden, wird ein Konflikt gemeldet. Die Datenbank bleibt im Konfliktfall in einem konsistenten Zustand. Der Konflikt ist nur am Client-Host sichtbar und muss dort gelöst werden.

29.1.2 rsync

Wenn Sie keine Versionskontrolle benötigen, aber große Dateistrukturen über langsame Netzwerkverbindungen synchronisieren möchten, bietet das Tool rsync ausgefeilte Mechanismen an, um ausschließlich Änderungen an Dateien zu übertragen. Dies betrifft nicht nur Textdateien sondern auch binäre Dateien. Um die Unterschiede zwischen Dateien zu erkennen, teilt rsync die Dateien in Blöcke auf und berechnet Prüfsummen zu diesen Blöcken.

Der Aufwand beim Erkennen der Änderungen hat seinen Preis. Für den Einsatz von rsync sollten die Computer, die synchronisiert werden sollen, großzügig dimensioniert sein. RAM ist besonders wichtig.

29.2 Kriterien für die Auswahl eines Programms

Bei der Entscheidung für ein Programm müssen einige wichtige Kriterien berücksichtigt werden.

29.2.1 Client-Server oder Peer-to-Peer

Zur Verteilung von Daten sind zwei verschiedene Modelle verbreitet. Im ersten Modell gleichen alle Clients ihre Dateien mit einem zentralen Server ab. Der Server muss zumindest zeitweise von allen Clients erreichbar sein. Dieses Modell wird von CVS verwendet.

Die andere Möglichkeit ist, dass alle Hosts gleichberechtigt (als Peers) vernetzt sind und ihre Daten gegenseitig abgleichen. rsync arbeitet eigentlich im Client-Modus, kann jedoch auch als Server ausgeführt werden.

29.2.2 Portabilität

CVS und rsync sind auch für viele andere Betriebssysteme, wie verschiedene Unix- und Windows-Systeme, erhältlich.

29.2.3 Interaktiv oder automatisch

In CVS startet der Benutzer die Datensynchronisierung manuell. Dies erlaubt die genaue Kontrolle über die abzugleichenden Dateien und einen einfachen Umgang mit Konflikten. Andererseits können sich durch zu lange Synchronisierungsintervalle die Chancen für Konflikte erhöhen.

29.2.4 Konflikte: Symptome und Lösungen

Konflikte treten in CVS nur selten auf, selbst wenn mehrere Leute an einem umfangreichen Programmprojekt arbeiten. Das liegt daran, dass die Dokumente zeilenweise zusammengeführt werden. Wenn ein Konflikt auftritt, ist davon immer nur ein Client betroffen. In der Regel lassen sich Konflikte in CVS einfach lösen.

In rsync gibt es keine Konfliktbehandlung. Der Benutzer muss selbst darauf achten, dass er nicht versehentlich Dateien überschreibt, und alle etwaigen Konflikte manuell lösen. Zur Sicherheit kann zusätzlich ein Versionssteuerungssystem wie RCS eingesetzt werden.

29.2.5 Auswählen und Hinzufügen von Dateien

In CVS müssen neue Verzeichnisse und Dateien explizit mit dem Befehl `cvs add` hinzugefügt werden. Daraus resultiert eine genauere Kontrolle über die zu synchronisierenden Dateien. Andererseits werden neue Dateien häufig übersehen, vor allem, wenn aufgrund einer großen Anzahl von Dateien die Fragezeichen in der Ausgabe von `cvs update` ignoriert werden.

29.2.6 Verlauf

CVS stellt zusätzlich die Funktion der Rekonstruktion alter Dateiversionen zur Verfügung. Bei jeder Änderung kann ein kurzer Bearbeitungsvermerk hinzugefügt werden. Damit lässt sich später die Entwicklung der Dateien aufgrund des Inhalts und der Vermerke gut nachvollziehen. Für Diplomarbeiten und Programmtexte ist dies eine wertvolle Hilfe.

29.2.7 Datenmenge und Speicherbedarf

Auf jedem der beteiligten Computer ist für alle verteilten Daten genügend Speicherplatz auf der Festplatte erforderlich. CVS benötigt zusätzlichen Speicherplatz für die Repository-Datenbank auf dem Server. Da auf dem Server auch die Datei-History gespeichert wird, ist dort deutlich mehr Speicherplatz nötig. Bei Dateien im Textformat müssen

nur geänderte Zeilen neu gespeichert werden. Bei binären Dateien wächst hingegen der Platzbedarf bei jeder Änderung um die Größe der Datei.

29.2.8 GUI

Erfahrene Benutzer führen CVS in der Regel über die Kommandozeile aus. Es sind jedoch grafische Bedienoberflächen für Linux (z. B. cervisia) und andere Betriebssysteme (z. B. wincvs) verfügbar. Viele Entwicklungswerkzeuge (z. B. kdevelop) und Texteditoren (z. B. emacs) unterstützen CVS. Die Behebung von Konflikten wird mit diesen Frontends oft sehr vereinfacht.

29.2.9 Benutzerfreundlichkeit

rsync ist einfach zu verwenden und auch für Neueinsteiger geeignet. CVS ist etwas weniger bedienerfreundlich. Benutzer sollten zu deren Verwendung das Zusammenspiel zwischen Repository und lokalen Daten verstehen. Änderungen der Daten sollten zunächst immer lokal mit dem Repository zusammengeführt werden. Hierzu wird der Befehl `cvs update` verwendet. Anschließend müssen die Daten über den Befehl cvs `commit` wieder in das Repository zurückgeschickt werden. Wenn dieser Vorgang verstanden wurde, können auch Einsteiger CVS mühelos verwenden.

29.2.10 Sicherheit vor Angriffen

Idealerweise sollten die Daten bei der Übertragung vor Abhören oder Änderungen geschützt sein. CVS und rsync lassen sich einfach über SSH (Secure Shell) benutzen und sind dann gut vor solchen Angriffen geschützt. Sie sollten CVS nicht über rsh (remote shell) ausführen. Zugriffe auf CVS mit dem Mechanismus *pserver* sind in ungeschützten Netzwerken ebenfalls nicht empfehlenswert.

29.2.11 Schutz vor Datenverlust

CVS wird schon sehr lange von vielen Entwicklern zur Verwaltung ihrer Programmprojekte benutzt und ist äußerst stabil. Durch das Speichern der Entwicklungsgeschichte bietet CVS sogar Schutz vor bestimmten Benutzerfehlern, wie irrtümliches Löschen einer Datei.

Tabelle 29.1 *Funktionen der Werkzeuge zur Dateisynchronisierung: -- = sehr schlecht, - = schlecht oder nicht verfügbar, o = mittel, + = gut, ++ = hervorragend, x = verfügbar*

	CVS	**rsync**
Client/Server	C-S	C-S
Portabilität	Lin,Un*x,Win	Lin,Un*x,Win
Interaktivität	x	x
Speed	o	+
Verursacht einen Konflikt	++	o
Dateiauswahl	Auswahl/file, dir.	Verz.
Verlauf	x	-
Speicherbedarf	--	o
GUI	o	-
Schwierigkeit	o	+
Angriffe	+ (ssh)	+(ssh)
Datenverlust	++	+

29.3 Einführung in CVS

CVS bietet sich zur Synchronisierung an, wenn einzelne Dateien häufig bearbeitet werden und in einem Dateiformat vorliegen, wie ASCII-Text oder Programmquelltext. Die Verwendung von CVS für die Synchronisierung von Daten in anderen Formaten (z. B. JPEG-Dateien) ist zwar möglich, führt aber schnell zu großen Datenmengen, da jede Variante einer Datei dauerhaft auf dem CVS-Server gespeichert wird. Zudem

bleiben in solchen Fällen die meisten Möglichkeiten von CVS ungenutzt. Die Verwendung von CVS zur Dateisynchronisierung ist nur möglich, wenn alle Arbeitsstationen auf denselben Server zugreifen können.

29.3.1 Konfigurieren eines CVS-Servers

Der *Server* ist der Ort, an dem sich alle gültigen Dateien befinden, einschließlich der neuesten Version jeder Datei. Jede stationäre Arbeitsstation kann als Server benutzt werden. Wünschenswert ist, dass die Daten des CVS-Repository in regelmäßige Backups einbezogen werden.

Beim Konigurieren eines CVS-Servers ist es sinnvoll, Benutzern über SSH Zugang zum Server zu gestatten. Ist auf diesem Server der Benutzer als `tux` bekannt und sowohl auf dem Server als auch auf dem Client die CVS-Software installiert, müssen auf der Client-Seite die folgenden Umgebungsvariablen gesetzt sein:

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

Mit dem Befehl `cvsinit` können Sie den CVS-Server von der Client-Seite aus initialisieren. Das ist nur einmal erforderlich.

Abschließend muss ein Name für die Synchronisierung festgelegt werden. Wählen oder erstellen Sie auf dem Client ein Verzeichnis für die Dateien, die von CVS verwaltet werden sollen (es darf auch leer sein). Der Name des Verzeichnisses ist auch der Name der Synchronisierung. In diesem Beispiel wird das Verzeichnis `synchome` genannt. Wechseln Sie in dieses Verzeichnis. Um den Synchronisationsnamen auf `synchome` zu setzen, geben Sie Folgendes ein:

```
cvs import synchome tux wilber
```

Viele Befehle von CVS erfordern einen Kommentar. Zu diesem Zweck startet CVS einen Editor (den in der Umgebungsvariable `$EDITOR` definierten, ansonsten vi). Den Aufruf des Editors können Sie umgehen, indem Sie den Kommentar bereits in der Kommandozeile eingeben, wie in folgendem Beispiel:

```
cvs import -m 'this is a test' synchome tux wilber
```

29.3.2 Verwenden von CSV

Das Synchronisierungsrepository kann jetzt mit `cvs co synchome` von allen Hosts aus gecheckt werden. Dadurch wird auf dem Client das neue Unterverzeichnis `synchome` angelegt. Um Ihre Änderungen an den Server zu übermitteln, wechseln Sie in das Verzeichnis `synchome` (oder eines seiner Unterverzeichnisse) und geben Sie `cvs commit` ein.

Standardmäßig werden alle Dateien (einschließlich Unterverzeichnisse) an den Server übermittelt. Um nur einzelne Dateien oder Verzeichnisse zu übermitteln, geben Sie diese folgendermaßen an: `cvs commit datei1 verzeichnis1`. Neue Dateien und Verzeichnisse müssen dem Repository mit einem Befehl wie `cvs add datei1 verzeichnis1` hinzugefügt werden, bevor sie an den Server übermittelt werden. Übermitteln Sie anschließend die neu hinzugefügten Dateien und Verzeichnisse mit `cvs commit datei1 verzeichnis1`.

Wenn Sie zu einer anderen Arbeitsstation wechseln, checken Sie das Synchronisierungsrepository aus, wenn nicht bereits in einer früheren Sitzung auf demselben Arbeitsplatzrechner geschehen.

Starten Sie die Synchronisierung mit dem Server über `cvs update`. Aktualisieren Sie einzelne Dateien oder Verzeichnisse, wie in `cvs update datei1 verzeichnis1`. Den Unterschied zwischen den aktuellen Dateien und den auf dem Server gespeicherten Versionen können Sie mit dem Befehl `cvs diff` oder `cvs diff datei1 verzeichnis1` anzeigen. Mit `cvs -nq update` können Sie anzeigen, welche Dateien von einer Aktualisierung betroffen sind.

Hier sind einige der Statussymbole, die während einer Aktualisierung angezeigt werden:

U
: Die lokale Version wurde aktualisiert. Dies betrifft alle Dateien, die vom Server bereitgestellt werden und auf dem lokalen System fehlen.

M
: Die lokale Version wurde geändert. Falls Änderungen am Server erfolgt sind, war es möglich, die Unterschiede mit der lokalen Kopie zusammenzuführen.

P
: Die lokale Version wurde durch einen Patch der Server-Version aktualisiert.

C
: Die lokale Datei hat einen Konflikt mit der aktuellen Version im Repository.

?
: Die Datei existiert nicht in CVS.

Der Status `M` kennzeichnet eine lokal geänderte Datei. Entweder übermitteln Sie die lokale Kopie an den Server oder Sie entfernen die lokale Datei und führen die Aktualisierung erneut durch. In diesem Fall wird die fehlende Datei vom Server abgerufen. Wenn von verschiedenen Benutzern die gleiche Datei in derselben Zeile editiert und dann übermittelt wurde, entsteht ein Konflikt, der mit `C` gekennzeichnet wird.

Beachten Sie in diesem Fall die Konfliktmarkierungen („>>“ und „<<“) in der Datei und entscheiden Sie sich für eine der beiden Versionen. Da diese Aufgabe unangenehm sein kann, können Sie Ihre Änderungen verwerfen, die lokale Datei löschen und mit der Eingabe `cvsup` die aktuelle Version vom Server abrufen.

29.4 Einführung in rsync

rsync bietet sich immer dann an, wenn große Datenmengen, die sich nicht wesentlich ändern, regelmäßig übertragen werden müssen. Dies ist z. B. bei der Erstellung von Sicherungskopien häufig der Fall. Ein weiteres Einsatzgebiet sind so genannte Staging-Server. Dabei handelt es sich um Server, auf denen komplette Verzeichnisstrukturen von Webservern gespeichert werden, die regelmäßig auf den eigentlichen Webserver in einer „DMZ“ gespiegelt werden.

29.4.1 Konfiguration und Betrieb

rsync lässt sich in zwei verschiedenen Modi benutzen. Zum einen kann rsync zum Archivieren oder Kopieren von Daten verwendet werden. Dazu ist auf dem Zielsystem nur eine Remote-Shell, wie z. B. SSH, erforderlich. Jedoch kann rsync auch als Daemon verwendet werden und Verzeichnisse im Netz zur Verfügung stellen.

Die grundlegende Verwendung von rsync erfordert keine besondere Konfiguration. Mit rsync ist es direkt möglich, komplette Verzeichnisse auf ein anderes System zu spiegeln. Beispielsweise kann mit folgendem Befehl ein Backup des Home-Verzeichnisses von "tux" auf einem Backupserver "sun" angelegt werden:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

Mit dem folgenden Befehl wird das Verzeichnis zurückgespielt:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Bis hierher unterscheidet sich die Benutzung kaum von einem normalen Kopierprogramm, wie scp.

Damit rsync seine Funktionen voll ausnutzen kann, sollte das Programm im „rsync"-Modus betrieben werden. Dazu wird auf einem der Systeme der Daemon rsyncd gestartet. Konfigurieren Sie rsync in der Datei `/etc/rsyncd.conf`. Wenn beispielsweise das Verzeichnis `/srv/ftp` über rsync zugänglich sein soll, verwenden Sie die folgende Konfiguration:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Starten Sie anschließend rsyncd mit `rcrsyncd start`. rsyncd kann auch automatisch beim Bootvorgang gestartet werden. Hierzu muss entweder dieser Dienst in YaST im Runlevel-Editor aktiviert oder manuell der Befehl `insserv rsyncd` eingegeben werden. Alternativ kann rsyncd auch von xinetd gestartet werden. Dies empfiehlt sich aber nur bei Servern, auf denen rsyncd nicht allzu oft verwendet wird.

Im obigen Beispiel wird auch eine Protokolldatei über alle Verbindungen angelegt. Diese Datei wird unter `/var/log/rsyncd.log` abgelegt.

Dann kann die Übertragung von einem Clientsystem aus getestet werden. Das geschieht mit folgendem Befehl:

```
rsync -avz sun::FTP
```

Dieser Befehl listet alle Dateien auf, die auf dem Server im Verzeichnis `/srv/ftp` liegen. Diese Anfrage wird auch in der Protokolldatei unter `/var/log/rsyncd.log` aufgezeichnet. Um die Übertragung tatsächlich zu starten, geben Sie ein Zielverzeichnis an. Verwenden Sie `.` für das aktuelle Verzeichnis. Beispiel:

```
rsync -avz sun::FTP .
```

Standardmäßig werden bei der Synchronisierung mit rsync keine Dateien gelöscht. Wenn dies erzwungen werden soll, muss zusätzlich die Option `--delete` angegeben werden. Um sicherzustellen, dass keine neueren Dateien überschrieben werden, kann stattdessen die Option `--update` angegeben werden. Dadurch entstehende Konflikte müssen manuell aufgelöst werden.

29.5 Weiterführende Informationen

CVS
: Wichtige Informationen zu CVS befinden sich auch auf der Homepage `http://www.cvshome.org`.

rsync
: Wichtige Informationen zu rsync finden Sie in den man-Seiten `manrsync` und `manrsyncd.conf`. Eine technische Dokumentation zur Vorgehensweise von rsync finden Sie unter `/usr/share/doc/packages/rsync/tech_report.ps`. Aktuelles zu rsync finden Sie auf der Projekt-Website unter `http://rsync.samba.org/`.



Teil V. Fehlersuche



30 Hilfe und Dokumentation

Im Lieferumfang von SUSE® Linux Enterprise Desktop sind verschiedene Informationen und Dokumentationen enthalten, viele davon bereits in Ihr installiertes System integriert.

Dokumentation unter `/usr/share/doc`
: Dieses traditionelle Hilfe-Verzeichnis enthält verschiedene Dokumentationsdateien sowie die Hinweise zur Version Ihres Systems. Außerdem enthält es Informationen über die im Unterverzeichnis `packages` installierten Pakete. Weitere Informationen finden Sie unter Abschnitt 30.1, „Dokumentationsverzeichnis“ (S. 450).

man-Seiten und Infoseiten für Shell-Kommandos
: Wenn Sie mit der Shell arbeiten, brauchen Sie die Optionen der Kommandos nicht auswendig zu kennen. Die Shell bietet normalerweise eine integrierte Hilfefunktion mit man-Seiten und Infoseiten. Weitere Informationen dazu finden Sie unter Abschnitt 30.2, „man-Seiten“ (S. 452) und Abschnitt 30.3, „Infoseiten“ (S. 453).

Desktop-Hilfezentren
: Die Hilfezentren sowohl des KDE-Desktops (KDE-Hilfezentrum) als auch des GNOME-Desktops (Yelp) bieten zentralen Zugriff auf die wichtigsten Dokumentationsressourcen auf Ihrem System in durchsuchbarer Form. Zu diesen Ressourcen zählen die Online-Hilfe für installierte Anwendungen, man-Seiten, Infoseiten sowie die mit Ihrem Produkt gelieferten Novell-/SUSE-Handbücher.

Separate Hilfepakete für einige Anwendungen
: Beim Installieren von neuer Software mit YaST wird die Software-Dokumentation in den meisten Fällen automatisch installiert und gewöhnlich in der Hilfe auf Ihrem Desktop angezeigt. Jedoch können einige Anwendungen, beispielsweise GIMP,

über andere Online-Hilfepakete verfügen, die separat mit YaST installiert werden können und nicht in die Hilfe integriert werden.

30.1 Dokumentationsverzeichnis

Das traditionelle Verzeichnis zum Suchen von Dokumentationen in Ihrem installierten Linux-System finden Sie unter `/usr/share/doc`. Das Verzeichnis enthält normalerweise Informationen zu den auf Ihrem System installierten Paketen sowie Versionshinweise, Handbücher usw.

ANMERKUNG: Inhalte abhängig von installierten Paketen

In der Linux-Welt stehen Handbücher und andere Dokumentationen in Form von Paketen zur Verfügung, ähnlich wie Software. Wie viele und welche Informationen Sie unter `/usr/share/docs` finden, hängt auch von den installierten (Dokumentations-) Paketen ab. Wenn Sie die hier genannten Unterverzeichnisse nicht finden können, prüfen Sie, ob die entsprechenden Pakete auf Ihrem System installiert sind, und fügen Sie sie gegebenenfalls mithilfe von YaST hinzu.

30.1.1 Novell-/SUSE-Handbücher

Wir bieten unsere Handbücher im HTML- und PDF-Format in verschiedenen Sprachen an. Im Unterverzeichnis `Handbuch` finden Sie HTML-Versionen der meisten für Ihr Produkt verfügbaren Novell-/SUSE-Handbücher. Eine Übersicht über sämtliche für Ihr Produkt verfügbare Dokumentation finden Sie im Vorwort der Handbücher.

Wenn mehr als eine Sprache installiert ist, enthält `/usr/share/doc/manual` möglicherweise verschiedene Sprachversionen der Handbücher. Die HTML-Versionen der Novell-/SUSE-Handbücher stehen auch in der Hilfe an beiden Desktops zur Verfügung. Informationen zum Speicherort der PDF- und HTML-Versionen des Handbuchs auf Ihrem Installationsmedium finden Sie in den Versionshinweisen zu SUSE Linux Enterprise Desktop. Sie stehen auf Ihrem installierten System unter `/usr/share/doc/release-notes/` oder online auf Ihrer produktspezifischen Webseite unter http://www.suse.com/doc/ zur Verfügung.

30.1.2 HOWTOs

Wenn das Paket `howto` auf Ihrem System installiert ist, enthält `/usr/share/doc` auch das Unterverzeichnis `howto` mit zusätzlicher Dokumentation zu vielen Aufgaben bei Setup und Betrieb von Linux-Software.

30.1.3 Dokumentation zu den einzelnen Paketen

Im Verzeichnis `packages` befindet sich die Dokumentation zu den auf Ihrem System installierten Software-Paketen. Für jedes Paket wird das entsprechende Unterverzeichnis `/usr/share/doc/packages/`*`Paketname`* erstellt. Es enthält README-Dateien für das Paket und manchmal Beispiele, Konfigurationsdateien und zusätzliche Skripten. In der folgenden Liste werden die typischen Dateien vorgestellt, die unter `/usr/share/doc/packages` zu finden sind. Diese Einträge sind nicht obligatorisch, und viele Pakete enthalten möglicherweise nur einige davon.

`AUTOREN`
: Liste der wichtigsten Entwickler.

`BUGS`
: Bekannte Programmfehler oder Fehlfunktionen. Enthält möglicherweise auch einen Link zur Bugzilla-Webseite, auf der alle Programmfehler aufgeführt sind.

`CHANGES` , `ChangeLog`
: Diese Datei enthält eine Übersicht der in den einzelnen Versionen vorgenommenen Änderungen. Die Datei dürfte nur für Entwickler interessant sein, da sie sehr detailliert ist.

`COPYING` , `LICENSE`
: Lizenzinformationen.

`FAQ`
: Mailing-Listen und Newsgroups entnommene Fragen und Antworten.

`INSTALL`
: So installieren Sie dieses Paket auf Ihrem System. Da das Paket bereits installiert ist, wenn Sie diese Datei lesen können, können Sie den Inhalt dieser Datei bedenkenlos ignorieren.

`README`, `README.*`
: Allgemeine Informationen zur Software, z. B. den Zweck und die Art ihrer Verwendung.

`TODO`
: Diese Datei beschreibt Funktionen, die in diesem Paket noch nicht implementiert, jedoch für spätere Versionen vorgesehen sind.

`MANIFEST`
: Diese Datei enthält eine Übersicht über die im Paket enthaltenen Dateien.

`NEWS`
: Beschreibung der Neuerungen in dieser Version.

30.2 man-Seiten

man-Seiten sind ein wichtiger Teil des Linux-Hilfesystems. Sie erklären die Verwendung der einzelnen Befehle und deren Optionen und Parameter. Sie greifen auf man-Seiten mit dem Befehl `man` gefolgt vom Namen des jeweiligen Befehls zu, z. B. `man ls`.

Die man-Seiten werden direkt in der Shell angezeigt. Blättern Sie mit den Tasten Bild ↑ und Bild ↓ nach oben bzw. unten. Mit Pos 1 und Ende gelangen Sie an den Anfang bzw. das Ende eines Dokuments. und mit Q schließen Sie die man-Seiten. Weitere Informationen über den Befehl `man` erhalten Sie durch Eingabe von `man man`. man-Seiten sind in Kategorien unterteilt, wie in Tabelle 30.1, „Manualpages – Kategorien und Beschreibungen“ (S. 453) gezeigt (diese Einteilung wurde direkt von der man-Seite für den Befehl „man“ übernommen).

Tabelle 30.1 Manualpages – Kategorien und Beschreibungen

Nummer	Beschreibung
1	Ausführbare Programme oder Shell-Befehle
2	Systemaufrufe (vom Kernel bereitgestellte Funktionen)
3	Bibliotheksaufrufe (Funktionen in Programmbibliotheken)
4	Spezielle Dateien (gewöhnlich in `/dev`)
5	Dateiformate und Konventionen (`/etc/fstab`)
6	Spiele
7	Sonstiges (wie Makropakete und Konventionen), zum Beispiel man(7) oder groff(7)
8	Systemverwaltungsbefehle (in der Regel nur für `root`)
9	Nicht standardgemäße Kernel-Routinen

Jede man-Seite besteht aus den Abschnitten *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* und *AUTHOR*. Je nach Befehlstyp stehen möglicherweise auch weitere Abschnitte zur Verfügung.

30.3 Infoseiten

Eine weitere wichtige Informationsquelle sind Infoseiten. Diese sind im Allgemeinen ausführlicher als man-Seiten. Die Infoseite für einen bestimmten Befehl zeigen Sie an,

indem Sie `info` gefolgt vom Namen des Befehls eingeben, z. B. `info ls`. Infoseiten werden direkt in der Shell in einem Viewer angezeigt, in dem Sie zwischen den verschiedenen Abschnitten, so genannten „Knoten, navigieren können“. Mit Leertaste blättern Sie vorwärts und mit <— zurück. Innerhalb eines Knotens können Sie auch mit Bild ↑ und Bild ↓ navigieren, jedoch gelangen Sie nur mit Leertaste und <— zum vorherigen bzw. nächsten Knoten. Drücken Sie Q, um den Anzeigemodus zu beenden. Nicht jede man-Seite enthält eine Infoseite und umgekehrt.

30.4 Online-Ressourcen

Zusätzlich zu den Online-Versionen der Novell-Handbücher, die unter `/usr/share/doc` installiert sind, können Sie auch auf die produktspezifischen Handbücher und Dokumentationen im Internet zugreifen. Eine Übersicht über alle Dokumentationen für SUSE Linux Enterprise Desktop finden Sie auf der produktspezifischen Dokumentations-Website unter http://www.suse.com/doc/.

Wenn Sie zusätzliche produktbezogene Informationen suchen, können Sie auch die folgenden Websites besuchen:

Novell Technischer Support – Wissensdatenbank
: Die Wissensdatenbank des Technischen Supports von Novell finden Sie unter http://www.novell.com/support/. Hier finden Sie Artikel mit Lösungen für technische Probleme mit SUSE Linux Enterprise Desktop.

Novell Foren
: Es gibt verschiedene Foren, in denen Sie sich an Diskussionen über Novell-Produkte beteiligen können. Eine Liste finden Sie in http://forums.novell.com/.

Cool Solutions
: Eine Online-Community, die Artikel, Tipps, Fragen und Antworten und kostenlose Tools zum Download bietet: http://www.novell.com/communities/coolsolutions

KDE-Dokumentation
: Eine Dokumentation zu vielen Aspekten von KDE für Benutzer und Administratoren finden Sie unter http://www.kde.org/documentation/.

GNOME-Dokumentation
: Dokumentation für GNOME-Benutzer, -Administratoren und -Entwickler finden Sie unter http://library.gnome.org/.

Das Linux-Dokumentationsprojekt
: Das Linux-Dokumentationsprojekt (TLDP) ist eine auf freiwilliger Mitarbeit beruhende Gemeinschaftsinitiative zur Erarbeitung von Linux-Dokumentationen und Veröffentlichungen zu verwandten Themen (siehe http://www.tldp.org). Dies ist die wahrscheinlich umfangreichste Dokumentationsressource für Linux. Sie finden dort durchaus Lernprogramme, die auch für Anfänger geeignet sind, doch hauptsächlich richten sich die Dokumente an erfahrene Benutzer, zum Beispiel an professionelle Systemadministratoren. Das Projekt veröffentlicht HOWTOs (Verfahrensbeschreibungen), FAQs (Antworten zu häufigen Fragen) sowie ausführliche Handbücher und stellt diese unter einer kostenlosen Lizenz zur Verfügung. Ein Teil der TLDP-Dokumentation ist auch unter SUSE Linux Enterprise Desktop verfügbar.

Sie können eventuell auch in den allgemeinen Suchmaschinen nachschlagen. Sie können beispielsweise die Suchbegriffe `Linux CD-RW Hilfe` oder `OpenOffice Dateikonvertierung` eingeben, wenn Sie Probleme mit dem Brennen von CDs bzw. mit der LibreOffice-Dateikonvertierung haben. Google™ bietet unter http://www.google.com/linux auch eine spezielle Linux-Suchmaschine, die nützlich sein kann.



Häufige Probleme und deren Lösung 31

In diesem Kapitel werden mögliche Probleme und deren Lösungen beschrieben. Auch wenn Ihre Situation nicht genau auf die hier beschriebenen Probleme zutreffen mag, finden Sie vielleicht einen ähnlichen Fall, der Ihnen Hinweise zur Lösung Ihres Problems liefert.

31.1 Suchen und Sammeln von Informationen

Linux gibt äußerst detailliert Aufschluss über die Vorgänge in Ihrem System. Es gibt mehrere Quellen, die Sie bei einem Problem mit Ihrem System zurate ziehen können. Einige davon beziehen sich auf Linux-Systeme im Allgemeinen, einige sind speziell auf SUSE Linux Enterprise Desktop-Systeme ausgerichtet. Die meisten Protokolldateien können mit YaST angezeigt werden (*Verschiedenes* > *Startprotokoll anzeigen*).

Mit YaST können Sie alle vom Support-Team benötigten Systeminformationen sammeln. Wählen Sie *Andere* > *Support* und dann die Kategorie Ihres Problems aus. Wenn alle Informationen gesammelt wurden, können Sie diese an Ihre Support-Anfrage anhängen.

Nachfolgend finden Sie eine Liste der wichtigsten Protokolldateien mit einer Beschreibung ihrer typischen Einsatzbereiche. Eine Tilde (~) in einer Pfadangabe verweist auf das Home-Verzeichnis des aktuellen Benutzers.

Tabelle 31.1 Protokolldateien

Protokolldatei	Beschreibung
`~/.xsession-errors`	Meldungen von den zurzeit ausgeführten Desktop-Anwendungen.
`/var/log/apparmor/`	Protokolldateien von AppArmor (Detailinformationen finden Sie unter Part “Confining Privileges with AppArmor” (↑*Security Guide*)).
`/var/log/audit/audit.log`	Protokolldatei von Audit, um Zugriffe auf Dateien, Verzeichnisse oder Ressourcen Ihres Systems sowie Systemaufrufe zu verfolgen.
`/var/log/boot.msg`	Meldungen vom Kernel beim Bootprozess.
`/var/log/mail.*`	Meldungen vom E-Mail-System.
`/var/log/messages`	Laufende Meldungen vom Kernel und dem Systemprotokoll-Daemon während der Ausführung.
`/var/log/NetworkManager`	NetworkManager-Protokolldatei zur Erfassung von Problemen hinsichtlich der Netzwerkkonnektivität
`/var/log/samba/`	Verzeichnis, das Protokollmeldungen vom Samba-Server und -Client enthält.
`/var/log/SaX.log`	Hardware-Meldungen von der SaX-Anzeige und dem KVM-System.
`/var/log/warn`	Alle Meldungen vom Kernel und dem Systemprotokoll-Daemon mit der Protokollstufe „Warnung“ oder höher.

Protokolldatei	Beschreibung
/var/log/wtmp	Binärdatei mit Benutzeranmeldedatensätzen für die aktuelle Computersitzung. Die Anzeige erfolgt mit `last`.
/var/log/Xorg.*.log	Unterschiedliche Start- und Laufzeitprotokolle des X-Window-Systems. Hilfreich für die Fehlersuche bei Problemen beim Start von X.
/var/log/YaST2/	Verzeichnis, das die Aktionen von YAST und deren Ergebnissen enthält.
/var/log/zypper.log	Protokolldatei von zypper.

Neben den Protokolldateien versorgt Ihr Computer Sie auch mit Informationen zum laufenden System. Weitere Informationen hierzu finden Sie unter Tabelle 31.2: Systeminformationen mit dem `/proc`-Dateisystem

Tabelle 31.2 *Systeminformationen mit dem /proc-Dateisystem*

Datei	Beschreibung
/proc/cpuinfo	Enthält Prozessorinformationen wie Typ, Fabrikat, Modell und Leistung.
/proc/dma	Zeigt die aktuell verwendeten DMA-Kanäle an.
/proc/interrupts	Zeigt an, welche Interrupts verwendet werden und wie viele bisher verwendet wurden.
/proc/iomem	Zeigt den Status des E/A (Eingabe/Ausgabe)-Speichers an.
/proc/ioports	Zeigt an, welche E/A-Ports zurzeit verwendet werden.

Datei	Beschreibung
/proc/meminfo	Zeigt den Speicherstatus an.
/proc/modules	Zeigt die einzelnen Module an.
/proc/mounts	Zeigt die zurzeit eingehängten Geräte an.
/proc/partitions	Zeigt die Partitionierung aller Festplatten an.
/proc/version	Zeigt die aktuelle Linux-Version an.

Abgesehen vom Dateisystem `/proc` exportiert der Linux-Kernel Informationen mit dem Modul `sysfs`, einem speicherinternen Dateisystem. Dieses Modul stellt Kernelobjekte, deren Attribute und Beziehungen dar. Weitere Informationen zu `sysfs` finden Sie im Kontext von udev im Abschnitt Kapitel 16, *Gerätemanagement über dynamischen Kernel mithilfe von* `udev` (S. 225). Tabelle 31.3 enthält einen Überblick über die am häufigsten verwendeten Verzeichnisse unter `/sys`.

***Tabelle 31.3** Systeminformationen mit dem /sys-Dateisystem*

Datei	Beschreibung
/sys/block	Enthält Unterverzeichnisse für jedes im System ermittelte Blockgerät. Im Allgemeinen handelt es sich dabei meistens um Geräte vom Typ Datenträger.
/sys/bus	Enthält Unterverzeichnisse für jeden physischen Bustyp.
/sys/class	Enthält Unterverzeichnisse, die nach den Funktionstypen der Geräte (wie Grafik, Netz, Drucker usw.) gruppiert sind.

Datei	Beschreibung
`/sys/device`	Enthält die globale Gerätehierarchie.

Linux bietet eine Reihe von Werkzeugen für die Systemanalyse und -überwachung. Unter Chapter 2, *System Monitoring Utilities* (↑*System Analysis and Tuning Guide*) finden Sie eine Auswahl der wichtigsten, die zur Systemdiagnose eingesetzt werden.

Jedes der nachfolgenden Szenarien beginnt mit einem Header, in dem das Problem beschrieben wird, gefolgt von ein oder zwei Absätzen mit Lösungsvorschlägen, verfügbaren Referenzen für detailliertere Lösungen sowie Querverweisen auf andere Szenarien, die mit diesem Szenario in Zusammenhang stehen.

31.2 Probleme bei der Installation

Probleme bei der Installation sind Situationen, wenn die Installation eines Computers nicht möglich ist. Der Vorgang kann entweder nicht ausgeführt oder das grafische Installationsprogramm nicht aufgerufen werden. In diesem Abschnitt wird auf einige typische Probleme eingegangen, die möglicherweise auftreten; außerdem finden Sie hier mögliche Lösungsansätze bzw. Tipps zur Umgehung solcher Fälle.

31.2.1 Überprüfen von Medien

Wenn Probleme bei der Verwendung des SUSE Linux Enterprise Desktop-Installationsmediums auftreten, können Sie die Integrität des Installationsmediums mit *Software* > *Medienprüfung* überprüfen. Datenträgerprobleme treten meist nur bei selbst gebrannten Datenträgern auf. Wenn Sie ein Installationsmedium von SUSE Linux Enterprise Desktop überprüfen möchten, legen Sie das Medium in das Laufwerk ein, und klicken Sie in YaST im Fenster *Medienprüfung* auf *Prüfvorgang starten*. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen. Wenn Fehler gefunden werden, sollten Sie dieses Medium nicht für die Installation verwenden.

Abbildung 31.1 *Überprüfen von Medien*

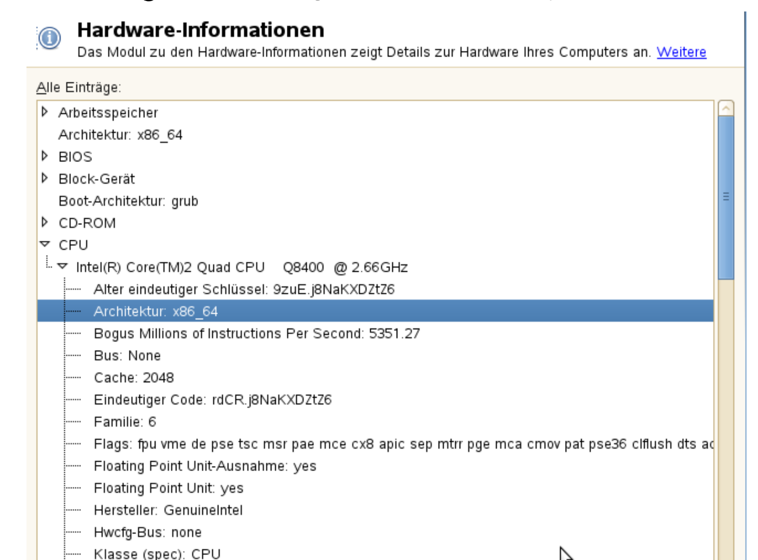


31.2.2 Hardware-Informationen

Die ermittelte Hardware und die technischen Daten können Sie über *Hardware* > *Hardware-Informationen* anzeigen. Klicken Sie auf einen beliebigen Knoten im Baum, um weitere Informationen zu einem Gerät zu erhalten. Dieses Modul ist besonders nützlich, wenn Sie eine Supportanforderung übermitteln, für die Angaben zur verwendeten Hardware erforderlich sind.

Die angezeigten Hardware-Informationen können Sie mit dem Befehl *In Datei speichern* in eine Datei speichern. Wählen Sie das gewünschte Verzeichnis und den gewünschten Dateinamen aus und klicken Sie auf *Speichern*, um die Datei zu erstellen.

Abbildung 31.2 *Anzeigen von Hardware-Informationen*



31.2.3 Kein bootfähiges DVD-Laufwerk verfügbar

Wenn Ihr Computer über kein bootfähiges DVD-ROM-Laufwerk verfügt bzw. das von Ihnen verwendete Laufwerk von Linux nicht unterstützt wird, gibt es mehrere Möglichkeiten zur Installation Ihres Computers ohne integriertem DVD-Laufwerk:

Booten von einer Diskette
: Erstellen Sie eine Bootdiskette und booten Sie von Diskette anstatt von DVD.

Verwenden eines externen Boot-Devices
: Wenn vom BIOS Ihres Computers und dem Installationskernel unterstützt, können Sie den Bootvorgang von einem externen DVD-Laufwerk ausführen.

Netzwerk-Boot über PXE
: Wenn ein Rechner kein DVD-Laufwerk aufweist, jedoch eine funktionierende Ethernet-Verbindung verfügbar ist, führen Sie eine vollständig netzwerkbasierte Installation durch. Details finden Sie unter Abschnitt „Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN“ (Kapitel 11, *Installation mit entferntem Zugriff*, ↑*Bereitstellungshandbuch*) und Abschnitt „Installation auf entfernten Systemen über SSH – PXE-Boot und Wake-on-LAN“ (Kapitel 11, *Installation mit entferntem Zugriff*, ↑*Bereitstellungshandbuch*).

31.2.3.1 Booten von einer Diskette (SYSLINUX)

Ältere Computer verfügen möglicherweise über kein bootfähiges DVD-Laufwerk, jedoch über ein Diskettenlaufwerk. Um die Installation auf einem System dieser Art vorzunehmen, erstellen Sie Bootdisketten und booten Sie Ihr System damit.

Die Bootdisketten enthalten den Loader SYSLINUX und das Programm linuxrc. SYSLINUX ermöglicht während der Bootprozedur die Auswahl eines Kernel sowie die Angabe sämtlicher Parameter, die für die verwendete Hardware erforderlich sind. Das linuxrc-Programm unterstützt das Landen von Kernel-Modulen für Ihre Hardware und startet anschließend die Installation.

Beim Booten von einer Bootdiskette wird die Bootprozedur vom Bootloader SYSLINUX initiiert (Paket `syslinux`). Wenn das System gebootet wird, führt SYSLINUX eine minimale Hardware-Erkennung durch, die hauptsächlich folgende Schritte umfasst:

1. Das Programm überprüft, ob das BIOS VESA 2.0-kompatible Framebuffer-Unterstützung bereitstellt, und bootet den Kernel entsprechend.

2. Die Überwachungsdaten (DDC info) werden gelesen.

3. Der erste Block der ersten Festplatte (MBR) wird gelesen, um bei der Bootloader-Konfiguration den Linux-Gerätenamen BIOS-IDs zuzuordnen. Das Programm ver-

sucht, den Block mithilfe der lba32-Funktionen des BIOS zu lesen, um zu ermitteln, ob das BIOS diese Funktionen unterstützt.

Wenn Sie beim Starten von SYSLINUX die Umschalttaste gedrückt halten, werden alle diese Schritte übersprungen. Fügen Sie für die Fehlersuche die Zeile

```
verbose 1
```

in `syslinux.cfg` ein, damit der Bootloader anzeigt, welche Aktion zurzeit ausgeführt wird.

Wenn der Computer nicht von der Diskette bootet, müssen Sie die Bootsequenz im BIOS möglicherweise in `A,C,CDROM` ändern.

31.2.3.2 Externe Boot-Devices

Linux unterstützt die meisten DVD-Laufwerke. Wenn das System kein DVD- bzw. Diskettenlaufwerk aufweist, kann ein externes, über USB, FireWire oder SCSI angeschlossenes DVD-Laufwerk zum Booten des Systems verwendet werden. Dies ist hauptsächlich von der Interaktion zwischen dem BIOS und der verwendeten Hardware abhängig. In einigen Fällen kann bei Problemen eine BIOS-Aktualisierung hilfreich sein.

31.2.4 Vom Installationsmedium kann nicht gebootet werden

Wenn ein Computer nicht vom Installationsmedium booten kann, ist im BIOS vermutlich eine falsche Boot-Sequenz eingestellt. In der BIOS-Boot-Sequenz muss das DVD-Laufwerk als erster Eintrag zum Booten festgelegt sein. Andernfalls versucht der Computer, von einem anderen Medium zu booten, normalerweise von der Festplatte. Anweisungen zum Ändern der BIOS-Boot-Sequenz finden Sie in der Dokumentation zu Ihrem Motherboard bzw. in den nachfolgenden Abschnitten.

Als BIOS wird die Software bezeichnet, die die absolut grundlegenden Funktionen eines Computers ermöglicht. Motherboard-Hersteller stellen ein speziell für ihre Hardware konzipiertes BIOS bereit. Normalerweise kann nur zu einem bestimmten Zeitpunkt auf das BIOS-Setup zugegriffen werden – wenn der Computer gebootet wird. Während dieser Initialisierungsphase führt der Computer einige Diagnosetests der Hardware durch. Einer davon ist die Überprüfung des Arbeitsspeichers, auf die durch

einen Arbeitsspeicherzähler hingewiesen wird. Wenn der Zähler eingeblendet wird, suchen Sie nach der Zeile, in der die Taste für den Zugriff auf das BIOS-Setup angegeben wird (diese Zeile befindet sich normalerweise unterhalb des Zählers oder am unteren Rand). In der Regel muss die Taste Entf, F1 oder Esc gedrückt werden. Halten Sie diese Taste gedrückt, bis der Bildschirm mit dem BIOS-Setup angezeigt wird.

Prozedur 31.1 *Ändern der BIOS-Bootsequenz*

1 Drücken Sie die aus den Bootroutinen hervorgehende Taste, um ins BIOS zu gelangen, und warten Sie, bis der BIOS-Bildschirm angezeigt wird.

2 Wenn Sie die Bootsequenz in einem AWARD BIOS ändern möchten, suchen Sie nach dem Eintrag *BIOS FEATURES SETUP* (SETUP DER BIOS-FUNKTIONEN). Andere Hersteller verwenden hierfür eine andere Bezeichnung, beispielsweise *ADVANCED CMOS SETUP* (ERWEITERTES CMOS-SETUP). Wenn Sie den Eintrag gefunden haben, wählen Sie ihn aus und bestätigen Sie ihn mit der Eingabetaste.

3 Suchen Sie im daraufhin angezeigten Bildschirm nach dem Untereintrag *BOOT SEQUENCE* (BOOTSEQUENZ) oder *BOOT ORDER* (BOOTREIHENFOLGE). Die Bootsequenz kann zum Beispiel `C,A` oder `A,C` lauten. Im ersten Fall durchsucht der Computer erst die Festplatte (C) und dann das Diskettenlaufwerk (A) nach einem bootfähigen Medium. Ändern Sie die Einstellungen mithilfe der Taste Bild-Auf bzw. Bild-Ab, bis die Sequenz `A,CDROM,C` lautet.

4 Drücken Sie Esc, um den BIOS-Setup-Bildschirm zu schließen. Zum Speichern der Änderungen wählen Sie *SAVE & EXIT SETUP* (SPEICHERN & SETUP BEENDEN) oder drücken Sie F10. Um zu bestätigen, dass Ihre Einstellungen gespeichert werden sollen, drücken Sie Y.

Prozedur 31.2 *Ändern der Bootsequenz in einem SCSI-BIOS (Adaptec-Hostadapter)*

1 Öffnen Sie das Setup, indem Sie die Tastenkombination Strg + A drücken.

2 Wählen Sie *Disk Utilities* (Festplattendienstprogramme) aus. Nun werden die angeschlossenen Hardwarekomponenten angezeigt.

Notieren Sie sich die SCSI-ID Ihres DVD-Laufwerks.

3 Verlassen Sie das Menü mit Esc.

4 Öffnen Sie *Configure Adapter Settings* (Adaptereinstellungen konfigurieren). Wählen Sie unter *Additional Options* (Zusätzliche Optionen) den Eintrag *Boot Device Options* (Boot-Device-Optionen) aus und drücken Sie die Eingabetaste.

5 Geben Sie die ID des DVD-Laufwerks ein und drücken Sie erneut die Eingabetaste.

6 Drücken Sie zweimal Esc, um zum Startbildschirm des SCSI-BIOS zurückzukehren.

7 Schließen Sie diesen Bildschirm und bestätigen Sie mit *Yes* (Ja), um den Computer zu booten.

Unabhängig von Sprache und Tastaturbelegung Ihrer endgültigen Installation wird in den meisten BIOS-Konfigurationen die US-Tastaturbelegung verwendet (siehe Abbildung):

Abbildung 31.3 *US-Tastaturbelegung*



31.2.5 Computer kann nicht gebootet werden

Bei bestimmter Hardware, insbesondere bei sehr alter bzw. sehr neuer, kann bei der Installation ein Fehler auftreten. In vielen Fällen ist dies darauf zurückzuführen, dass dieser Hardwaretyp im Installationskernel noch nicht oder nicht mehr unterstützt wird; oft führen auch bestimmte Funktionen dieses Kernel, beispielsweise ACPI (Advanced Configuration and Power Interface), bei bestimmter Hardware zu Problemen.

Wenn Ihr System über den standardmäßigen Modus für die *Installation* (Installation) im ersten Installations-Bootbildschirm nicht installiert werden kann, gehen Sie folgendermaßen vor:

1 Belassen Sie die DVD im Laufwerk und booten Sie den Computer über die Tastenkombination Strg + Alt + Entf bzw. über den Reset-Knopf der Hardware neu.

2 Drücken Sie, sobald der Boot-Bildschirm angezeigt wird, auf F5, navigieren Sie mithilfe der Pfeiltasten der Tastatur zu *Kein ACPI* und drücken Sie die Eingabetaste, um den Boot- und Installationsvorgang zu starten. Mit dieser Option wird die Unterstützung für ACPI-Energieverwaltungstechniken deaktiviert.

3 Fahren Sie wie in Kapitel 3, *Installation mit YaST* (↑*Bereitstellungshandbuch*) beschrieben mit der Installation fort.

Wenn es hierbei zu Problemen kommt, fahren Sie wie oben beschrieben fort, wählen Sie jedoch in diesem Fall *Sichere Einstellungen* aus. Mit dieser Option wird die Unterstützung für ACPI und DMA (Direct Memory Access) deaktiviert. Mit dieser Option kann die meiste Hardware gebootet werden.

Wenn bei diesen beiden Optionen Probleme auftauchen, versuchen Sie mithilfe der Bootoptionen-Eingabeaufforderung sämtliche zusätzlichen Parameter, die für die Unterstützung dieses Hardwaretyps erforderlich sind, an den Installationskernel zu übermitteln. Weitere Informationen zu den Parametern, die als Bootoptionen zur Verfügung stehen, finden Sie in der Kernel-Dokumentation unter `/usr/src/linux/Documentation/kernel-parameters.txt`.

TIPP: Aufrufen der Kernel-Dokumentation

Installieren Sie das Paket `kernel-source`. Darin ist die Kernel-Dokumentation enthalten.

Es gibt noch einige andere mit ACPI in Zusammenhang stehende Kernel-Parameter, die vor dem Booten zu Installationszwecken an der Booteingabeaufforderung eingegeben werden können:

`acpi=off`
: Mit diesem Parameter wird das vollständige ACPI-Subsystem auf Ihrem Computer deaktiviert. Dies kann hilfreich sein, wenn ACPI von Ihrem Computer nicht unterstützt wird bzw. Sie vermuten, dass ACPI auf Ihrem Computer zu Problemen führt.

`acpi=force`
: Aktivieren Sie ACPI in jedem Fall, auch wenn das BIOS Ihres Computers von vor dem Jahre 2000 stammt. Mit diesem Parameter wird ACPI auch aktiviert, wenn die Festlegung zusätzlich zu `acpi=off` erfolgt.

`acpi=noirq`
: ACPI nicht für IRQ-Routing verwenden.

`acpi=ht`
: Nur genügend ACPI ausführen, um Hyper-Threading zu aktivieren.

`acpi=strict`
: Geringere Toleranz von Plattformen, die nicht genau der ACPI-Spezifikation entsprechen.

`pci=noacpi`
: Deaktiviert das PCI-IRQ-Routing des neuen ACPI-Systems.

`pnpacpi=off`
: Diese Option ist für Probleme mit seriellen oder parallelen Ports vorgesehen, wenn Ihr BIOS-Setup falsche Interrupts oder Ports enthält.

`notsc`
: Hiermit wird der Zeitstempelzähler deaktiviert. Diese Option dient der Umgehung von Timing-Problemen auf Ihren Systemen. Es handelt sich um eine recht neue Funktion, die insbesondere dann nützlich sein kann, wenn Sie auf Ihrem Rechner Rückwärtsentwicklungen bemerken, insbesondere zeitbezogene Rückwärtsentwicklungen. Gilt auch für Fälle, in denen keinerlei Reaktion mehr zu verzeichnen ist.

`nohz=off`
: Hiermit wird die nohz-Funktion deaktiviert. Wenn der Rechner nicht mehr reagiert, ist diese Option vielleicht die Lösung. Andernfalls wird sie Ihnen kaum nützlich sein.

Nachdem Sie die richtige Parameterkombination ermittelt haben, schreibt YaST sie automatisch in die Bootloader-Konfiguration, um sicherzustellen, dass das System beim nächsten Mal vorschriftsmäßig gebootet wird.

Wenn beim Laden des Kernel oder bei der Installation unerwartete Fehler auftreten, wählen Sie im Bootmenü die Option *Memory Test* (Speichertest), um den Arbeitsspeicher

zu überprüfen. Wenn von *Memory Test* (Speichertest) ein Fehler zurückgegeben wird, liegt in der Regel ein Hardware-Fehler vor.

31.2.6 Grafisches Installationsprogramm lässt sich nicht starten

Nachdem Sie das Medium in das Laufwerk eingelegt und den Computer neu gebootet haben, wird der Installationsbildschirm angezeigt, nach der Auswahl von *Installation* wird jedoch das grafische Installationsprogramm nicht aufgerufen.

In diesem Fall haben Sie mehrere Möglichkeiten:

- Wählen Sie eine andere Bildschirmauflösung für die installationsbezogenen Dialogfelder.
- Wählen Sie den *Text Mode* (Expertenmodus) für die Installation aus.
- Führen Sie über VNC und unter Verwendung des grafischen Installationsprogramms eine entfernte Installation durch.

Prozedur 31.3 *Ändern der Bildschirmauflösung für die Installation*

1 Booten Sie zu Installationszwecken.

2 Drücken Sie F3, um ein Menü zu öffnen, in dem Sie für Installationszwecke eine niedrigere Auflösung auswählen können.

3 Wählen Sie *Installation* aus und fahren Sie, wie in Kapitel 3, *Installation mit YaST* (↑*Bereitstellungshandbuch*) beschrieben, mit der Installation fort.

Prozedur 31.4 *Installation im Textmodus*

1 Booten Sie zu Installationszwecken.

2 Drücken Sie F3 und wählen Sie *Text Mode* (Expertenmodus) aus.

3 Wählen Sie *Installation* aus und fahren Sie, wie in Kapitel 3, *Installation mit YaST* (↑*Bereitstellungshandbuch*) beschrieben, mit der Installation fort.

Prozedur 31.5 *VNC-Installation*

1 Booten Sie zu Installationszwecken.

2 Geben Sie an der Bootoptionen-Eingabeaufforderung folgenden Text ein:

```
vnc=1 vncpassword=some_password
```

Ersetzen Sie *beliebiges_passwort* durch das für die VNC-Installation zu verwendende Passwort.

3 Wählen Sie *Installation* (Installation) aus und drücken Sie dann die Eingabetaste, um die Installation zu starten.

Anstatt direkt in die Routine für die grafische Installation einzusteigen, wird das System weiterhin im Textmodus ausgeführt und dann angehalten; in einer Meldung werden die IP-Adresse und die Portnummer angegeben, unter der über die Browserschnittstelle oder eine VNC-Viewer-Anwendung auf das Installationsprogramm zugegriffen werden kann.

4 Wenn Sie über einen Browser auf das Installationsprogramm zugreifen, starten Sie den Browser, geben Sie die Adressinformationen ein, die von den Installationsroutinen auf dem zukünftigen SUSE Linux Enterprise Desktop-Computer bereitgestellt werden, und drücken Sie die Eingabetaste:

```
http://ip_address_of_machine:5801
```

Im Browserfenster wird ein Dialogfeld geöffnet, in dem Sie zur Eingabe des VNC-Passworts aufgefordert werden. Geben Sie das Passwort ein und fahren Sie, wie in Kapitel 3, *Installation mit YaST* (↑*Bereitstellungshandbuch*) beschrieben, mit der Installation fort.

WICHTIG

Die Installation über VNC kann mit jedem Browser und unter jedem beliebigen Betriebssystem vorgenommen werden, vorausgesetzt, die Java-Unterstützung ist aktiviert.

Geben Sie auf Aufforderung die IP-Adresse und das Passwort für Ihren VNC-Viewer ein. Daraufhin wird ein Fenster mit den installationsbezogenen Dialogfeldern geöffnet. Fahren Sie wie gewohnt mit der Installation fort.

31.2.7 Nur ein minimalistischer Bootbildschirm wird eingeblendet

Sie haben das Medium in das Laufwerk eingelegt, die BIOS-Routinen sind abgeschlossen, das System zeigt jedoch den grafischen Bootbildschirm nicht an. Stattdessen wird eine sehr minimalistische textbasierte Oberfläche angezeigt. Dies kann auf Computern der Fall sein, die für die Darstellung eines grafischen Bootbildschirms nicht ausreichend Grafikspeicher aufweisen.

Obwohl der textbasierte Bootbildschirm minimalistisch wirkt, bietet er nahezu dieselbe Funktionalität wie der grafische:

Bootoptionen
: Im Gegensatz zur grafischen Oberfläche können die unterschiedlichen Bootoptionen nicht mithilfe der Cursortasten der Tastatur ausgewählt werden. Das Bootmenü des Expertenmodus-Bootbildschirms ermöglicht die Eingabe einiger Schlüsselwörter an der Booteingabeaufforderung. Diese Schlüsselwörter sind den Optionen in der grafischen Version zugeordnet. Treffen Sie Ihre Wahl und drücken Sie die Eingabetaste, um den Bootprozess zu starten.

Benutzerdefinierte Bootoptionen
: Geben Sie nach der Auswahl einer Bootoption das entsprechende Schlüsselwort an der Booteingabeaufforderung ein. Sie können auch einige benutzerdefinierte Bootoptionen eingeben (siehe Abschnitt 31.2.5, „Computer kann nicht gebootet werden“ (S. 467)). Wenn Sie den Installationsvorgang starten möchten, drücken Sie die Eingabetaste.

Bildschirmauflösungen
: Die Bildschirmauflösung für die Installation lässt sich mithilfe der F-Tasten bestimmen. Wenn Sie im Expertenmodus, also im Textmodus, booten müssen, drücken Sie F3.

31.3 Probleme beim Booten

Probleme beim Booten sind Fälle, in denen Ihr System nicht vorschriftsmäßig gebootet wird, das Booten also nicht mit dem erwarteten Runlevel und Anmeldebildschirm erfolgt.

31.3.1 Probleme beim Laden des GRUB -Bootloaders

Wenn die Hardware vorschriftsmäßig funktioniert, ist möglicherweise der Bootloader beschädigt und Linux kann auf dem Computer nicht gestartet werden. In diesem Fall muss der Bootloader neu installiert werden. Gehen Sie zur erneuten Installation des Bootloader wie folgt vor:

1. Legen Sie das Installationsmedium in das Laufwerk ein.

2. Booten Sie den Computer neu.

3. Wählen Sie im Bootmenü die Option *Installation* (Installation) aus.

4. Wählen Sie eine Sprache aus.

5. Nehmen Sie die Lizenzvereinbarung an.

6. Wählen Sie auf dem Bildschirm *Installationsmodus* die Option *Reparatur des installierten Systems* aus.

7. Wenn Sie sich im YaST-Modul für die Systemreparatur befinden, wählen Sie zunächst *Expertenwerkzeuge* und dann *Neuen Bootloader installieren* aus.

8. Stellen Sie die ursprünglichen Einstellungen wieder her und installieren Sie den Bootloader neu.

9. Beenden Sie die YaST-Systemreparatur und booten Sie das System neu.

Die Grunde dafür, dass der Computer nicht gebootet werden kann, stehen möglicherweise in Zusammenhang mit dem BIOS.

BIOS-Einstellungen
: Überprüfen Sie Ihr BIOS auf Verweise auf Ihre Festplatte hin. GRUB wird möglicherweise einfach deshalb nicht gestartet, weil die Festplatte bei den aktuellen BIOS-Einstellungen nicht gefunden wird.

BIOS-Bootreihenfolge
: Überprüfen Sie, ob die Festplatte in der Bootreihenfolge Ihres Systems enthalten ist. Wenn die Festplatten-Option nicht aktiviert wurde, wird Ihr System möglicherweise vorschriftsmäßig installiert. Das Booten ist jedoch nicht möglich, wenn auf die Festplatte zugegriffen werden muss.

31.3.2 Es wird keine Anmeldemaske oder Eingabeaufforderung angezeigt

Dieses Verhalten tritt normalerweise nach einer nicht erfolgreichen Kernelaufrüstung auf und ist nach der Art von Fehler auf der Systemkonsole, der zuweilen im Endstadium des Vorgangs auftritt, als *Kernelpanik* bekannt. Wenn der Computer tatsächlich soeben nach einer Softwareaktualisierung neu gebootet wurde, sollte er zunächst mithilfe der alten, bewährten Version des Linux-Kernels und der zugehörigen Dateien erneut gebootet werden. Gehen Sie dazu während des Bootvorgangs im Bildschirm des GRUB-Bootloaders wie folgt vor:

1. Booten Sie den Computer mithilfe der Schaltfläche zum Zurücksetzen neu oder schalten Sie ihn aus und wieder an.

2. Wenn der GRUB-Bootbildschirm angezeigt wird, wählen Sie *Linux--Failsafe* aus und drücken Sie dann die Eingabetaste. Der Computer sollte nun mithilfe der früheren Version des Kernels und der zugehörigen Dateien gebootet werden.

3. Entfernen Sie nach Abschluss des Bootvorgangs den neu installierten Kernel und bearbeiten Sie, falls erforderlich, die Datei `/boot/grub/menu.lst` manuell, um den älteren Kernel as Standardoption anzugeben. Detailliertere Informationen zu der in dieser Konfigurationsdatei verwendeten Syntax finden Sie in Kapitel 12, *Der Bootloader GRUB* (S. 151).

   Möglicherweise ist eine Aktualisierung dieser Datei nicht erforderlich, da sie normalerweise während des Rollback-Vorgangs von den automatischen Aktualisierungswerkzeugen bearbeitet wird.

4. Booten Sie den Computer neu.

Wenn sich das Problem dadurch nicht lösen lässt, da der Computer mit der Option *Linux--Failsafe* nicht ordnungsgemäß gebootet wird, booten Sie den Computer mithilfe

des Installationsdatenträgers. Fahren Sie nach dem Booten des Computers mit Schritt 3 (S. 474) und fort.

31.3.3 Keine grafische Anmeldung

Wenn der Computer hochfährt, jedoch der grafische Anmelde-Manager nicht gebootet wird, müssen Sie entweder hinsichtlich der Auswahl des standardmäßigen Runlevel oder der Konfiguration des X-Window-Systems mit Problemen rechnen. Wenn Sie die Runlevel-Konfiguration überprüfen möchten, melden Sie sich als `root`-Benutzer an und überprüfen Sie, ob der Computer so konfiguriert ist, dass das Booten in Runlevel 5 erfolgt (grafischer Desktop). Eine schnelle Möglichkeit stellt das Überprüfen des Inhalts von `/etc/inittab` dar, und zwar folgendermaßen:

```
tux@mercury:~> grep "id:" /etc/inittab
id:5:initdefault:
```

Aus der zurückgegebenen Zeile geht hervor, dass der Standard-Runlevel des Computer (`initdefault`) auf `5` eingestellt ist und dass das Booten in den grafischen Desktop erfolgt. Wenn der Runlevel auf eine andere Nummer eingestellt ist, kann er über den YaST-Runlevel-Editor auf `5` eingestellt werden.

WICHTIG

Bearbeiten Sie die Runlevel-Konfiguration nicht manuell. Andernfalls überschreibt SUSEconfig (durch YaST ausgeführt) diese Änderungen bei der nächsten Ausführung. Wenn Sie hier manuelle Änderungen vornehmen möchten, deaktivieren Sie zukünftige Änderungen, indem Sie *`CHECK_INITTAB`* in `/etc/sysconfig/suseconfig` auf `no` (Nein) festlegen.

Wenn Runlevel auf `5` gesetzt ist, ist vermutlich Ihre Desktop- oder X Windows-Software falsch konfiguriert oder beschädigt. Suchen Sie in den Protokolldateien von `/var/log/Xorg.*.log` nach detaillierten Meldungen vom X-Server beim versuchten Start. Wenn es beim Starten zu einem Problem mit dem Desktop kommt, werden möglicherweise Fehlermeldungen in `/var/log/messages` protokolliert. Wenn diese Fehlermeldungen auf ein Konfigurationsproblem mit dem X-Server hinweisen, versuchen Sie, diese Probleme zu beseitigen. Wenn das grafische System weiterhin nicht aktiviert wird, ziehen Sie die Neuinstallation des grafischen Desktop in Betracht.

TIPP: Manueller Start von X Window System

Schneller Test: Durch das Kommando `startx` sollte das X-Windows-System mit den konfigurierten Standardeinstellungen gestartet werden, wenn der Benutzer derzeit bei der Konsole angemeldet ist. Wenn dies nicht funktioniert, sollten Fehler auf der Konsole protokolliert werden.

31.4 Probleme bei der Anmeldung

Probleme bei der Anmeldung sind Fälle, in denen Ihr Computer in den erwarteten Begrüßungsbildschirm bzw. die erwartete Anmelde-Eingabeaufforderung bootet, den Benutzernamen und das Passwort jedoch entweder nicht akzeptiert oder zunächst akzeptiert, sich dann aber nicht erwartungsgemäß verhält (der grafische Desktop wird nicht gestartet, es treten Fehler auf, es wird wieder eine Kommandozeile angezeigt usw.).

31.4.1 Benutzer kann sich trotz gültigem Benutzernamen und Passwort nicht anmelden

Dieser Fall tritt normalerweise ein, wenn das System zur Verwendung von Netzwerkauthentifizierung oder Verzeichnisdiensten konfiguriert wurde und aus unbekannten Gründen keine Ergebnisse von den zugehörigen konfigurierten Servern abrufen kann. Der `root`-Benutzer ist der einzige lokale Benutzer, der sich noch bei diesen Computern anmelden kann. Nachfolgend sind einige häufige Ursachen dafür aufgeführt, weshalb Anmeldungen nicht ordnungsgemäß verarbeitet werden können, obwohl der Computer funktionstüchtig zu sein scheint:

- Es liegt ein Problem mit der Netzwerkfunktion vor. Weitere Anweisungen hierzu finden Sie in Abschnitt 31.5, „Probleme mit dem Netzwerk“ (S. 485).

- DNS ist zurzeit nicht funktionsfähig (dadurch ist GNOME bzw. KDE nicht funktionsfähig und das System kann keine an sichere Server gerichteten bestätigten Anforderungen durchführen). Ein Hinweis, dass dies zutrifft, ist, dass der Computer

auf sämtliche Aktionen ausgesprochen langsam reagiert. Weitere Informationen zu diesem Thema finden Sie in Abschnitt 31.5, „Probleme mit dem Netzwerk“ (S. 485).

- Wenn das System für die Verwendung von Kerberos konfiguriert ist, hat die lokale Systemzeit möglicherweise die zulässige Abweichung zur Kerberos-Serverzeit (üblicherweise 300 Sekunden) überschritten. Wenn NTP (Network Time Protocol) nicht ordnungsgemäß funktioniert bzw. lokale NTP-Server nicht funktionieren, kann auch die Kerberos-Authentifizierung nicht mehr verwendet werden, da sie von der allgemeinen netzwerkübergreifenden Uhrsynchronisierung abhängt.

- Die Authentifizierungskonfiguration des Systems ist fehlerhaft. Prüfen Sie die betroffenen PAM-Konfigurationsdateien auf Tippfehler oder falsche Anordnung von Direktiven hin. Zusätzliche Hintergrundinfomationen zu PAM (Password Authentification Module) und der Syntax der betroffenen Konfigurationsdateien finden Sie in Chapter 2, *Authentication with PAM* (↑*Security Guide*).

- Die Home-Partition ist verschlüsselt. Weitere Informationen zu diesem Thema finden Sie in Abschnitt 31.4.3, „Anmeldung bei verschlüsselter Home-Partition fehlgeschlagen“ (S. 481).

In allen Fällen, in denen keine externen Netzwerkprobleme vorliegen, besteht die Lösung darin, das System erneut im Einzelbenutzermodus zu booten und die Konfigurationsfehler zu beseitigen, bevor Sie erneut in den Betriebsmodus booten und erneut versuchen, sich anzumelden. So booten Sie in den Einzelbenutzerbetrieb:

1 Booten Sie das System neu. Daraufhin wird der Bootbildschirm mit einer Eingabeaufforderung eingeblendet.

2 Geben Sie an der Booteingabeaufforderung `1` ein, damit das System in den Einzelbenutzerbetrieb bootet.

3 Geben Sie Benutzername und Passwort für `root` ein.

4 Nehmen Sie alle erforderlichen Änderungen vor.

5 Booten Sie in den vollen Mehrbenutzer- und Netzwerkbetrieb, indem Sie `telinit 5` an der Kommandozeile eingeben.

31.4.2 Gültiger Benutzername/gültiges Passwort werden nicht akzeptiert

Dies ist das mit Abstand häufigste Problem, auf das Benutzer stoßen, da es hierfür zahlreiche Ursachen gibt. Je nachdem, ob Sie lokale Benutzerverwaltung und Authentifizierung oder Netzwerkauthentifizierung verwenden, treten Anmeldefehler aus verschiedenen Gründen auf.

Fehler bei der lokalen Benutzerverwaltung können aus folgenden Gründen auftreten:

- Der Benutzer hat möglicherweise das falsche Passwort eingegeben.
- Das Home-Verzeichnis des Benutzers, das die Desktopkonfigurationsdateien enthält, ist beschädigt oder schreibgeschützt.
- Möglicherweise bestehen hinsichtlich der Authentifizierung dieses speziellen Benutzers durch das X Windows System Probleme, insbesondere, wenn das Home-Verzeichnis des Benutzers vor der Installation der aktuellen Distribution für andere Linux-Distributionen verwendet wurde.

Gehen Sie wie folgt vor, um den Grund für einen Fehler bei der lokalen Anmeldung ausfindig zu machen:

1. Überprüfen Sie, ob der Benutzer sein Passwort richtig in Erinnerung hat, bevor Sie mit der Fehlersuche im gesamten Authentifizierungsmechanismus beginnen. Sollte sich der Benutzer nicht mehr an sein Passwort erinnern, können Sie es mithilfe des YaST-Moduls für die Benutzerverwaltung ändern. Achten Sie auf die Feststelltaste und deaktivieren Sie sie gegebenenfalls.

2. Melden Sie sich als `root`-Benutzer an und untersuchen Sie `/var/log/messages` auf PAM-Fehlermeldungen und Fehlermeldungen aus dem Anmeldeprozess.

3. Versuchen Sie, sich von der Konsole aus anzumelden (mit Strg + Alt + F1). Wenn dies gelingt, liegt der Fehler nicht bei PAM, da die Authentifizierung dieses Benutzers auf diesem Computer möglich ist. Versuchen Sie, mögliche Probleme mit dem X-Window-System oder dem Desktop (GNOME bzw. KDE) zu ermitteln. Weitere Informationen finden Sie in Abschnitt 31.4.4, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“ (S. 482) und Abschnitt 31.4.5, „Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop“ (S. 483).

4 Wenn das Home-Verzeichnis des Benutzers für eine andere Linux-Distribution verwendet wurde, entfernten Sie die Datei `Xauthority` aus dem Heimverzeichnis des Benutzers. Melden Sie sich von der Konsole aus mit Strg + Alt + F1 an und führen Sie `rm .Xauthority` als diesen Benutzer aus. Auf diese Weise sollten die X-Authentifizierungsprobleme dieses Benutzers beseitigt werden. Versuchen Sie erneut, sich beim grafischen Desktop anzumelden.

5 Wenn die grafikbasierte Anmeldung nicht möglich ist, melden Sie sich mit Strg + Alt + F1 bei der Konsole an. Versuchen Sie, eine X-Sitzung in einer anderen Anzeige zu starten; die erste (`:0`) wird bereits verwendet:

```
startx -- :1
```

Daraufhin sollten ein grafikbasierter Bildschirm und Ihr Desktop angezeigt werden. Prüfen Sie andernfalls die Protokolldateien des X-Window-Systems (`/var/log/Xorg.`*`anzeigennummer`*`.log`) bzw. die Protokolldateien Ihrer Desktop-Anwendungen (`.xsession-errors` im Home-Verzeichnis des Benutzers) auf Unregelmäßigkeiten hin.

6 Wenn der Desktop aufgrund beschädigter Konfigurationsdateien nicht aufgerufen werden konnte, fahren Sie mit Abschnitt 31.4.4, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“ (S. 482) oder Abschnitt 31.4.5, „Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop“ (S. 483) fort.

Nachfolgend sind einige häufige Ursachen dafür aufgeführt, weshalb es bei der Netzwerkauthentifizierung eines bestimmten Benutzers auf einem bestimmten Computer zu Problemen kommen kann:

- Der Benutzer hat möglicherweise das falsche Passwort eingegeben.

- Der Benutzername ist in den lokalen Authentifizierungsdateien des Computers vorhanden und wird zudem von einem Netzwerkauthentifizierungssystem bereitgestellt, was zu Konflikten führt.

- Das Home-Verzeichnis ist zwar vorhanden, ist jedoch beschädigt oder nicht verfügbar. Es ist möglicherweise schreibgeschützt oder befindet sich auf einem Server, auf den momentan nicht zugegriffen werden kann.

- Der Benutzer ist nicht berechtigt, sich bei diesem Host im Authentifizierungssystem anzumelden.

- Der Hostname des Computers hat sich geändert und der Benutzer ist nicht zur Anmeldung bei diesem Host berechtigt.

- Der Computer kann keine Verbindung mit dem Authentifizierungs- oder Verzeichnisserver herstellen, auf dem die Informationen dieses Benutzers gespeichert sind.

- Möglicherweise bestehen hinsichtlich der Authentifizierung dieses speziellen Benutzers durch das X Window System Probleme, insbesondere, wenn das Home-Verzeichnis des Benutzers vor der Installation der aktuellen Distribution für andere Linux-Distributionen verwendet wurde.

Gehen Sie wie folgt vor, um die Ursache der Anmeldefehler bei der Netzwerkauthentifizierung zu ermitteln:

1. Überprüfen Sie, ob der Benutzer sein Passwort richtig in Erinnerung hat, bevor Sie mit der Fehlersuche im gesamten Authentifizierungsmechanismus beginnen.

2. Ermitteln Sie den Verzeichnisserver, den der Computer für die Authentifizierung verwendet, und vergewissern Sie sich, dass dieser ausgeführt wird und ordnungsgemäß mit den anderen Computern kommuniziert.

3. Überprüfen Sie, ob der Benutzername und das Passwort des Benutzers auf anderen Computern funktionieren, um sicherzustellen, dass seine Authentifizierungsdaten vorhanden sind und ordnungsgemäß verteilt wurden.

4. Finden Sie heraus, ob sich ein anderer Benutzer bei dem problembehafteten Computer anmelden kann. Wenn sich ein anderer Benutzer oder der `root`-Benutzer anmelden kann, melden Sie sich mit dessen Anmeldedaten an und überprüfen Sie die Datei `/var/log/messages`. Suchen Sie nach dem Zeitstempel, der sich auf die Anmeldeversuche bezieht, und finden Sie heraus, ob von PAM Fehlermeldungen generiert wurden.

5. Versuchen Sie, sich von der Konsole aus anzumelden (mit Strg + Alt + F1). Wenn dies gelingt, liegt der Fehler nicht bei PAM oder dem Verzeichnisserver mit dem Home-Verzeichnis des Benutzers, da die Authentifizierung dieses Benutzers auf diesem Computer möglich ist. Versuchen Sie, mögliche Probleme mit dem X-Window-System oder dem Desktop (GNOME bzw. KDE) zu ermitteln. Weitere Informationen finden Sie in Abschnitt 31.4.4, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“ (S. 482) und Abschnitt 31.4.5, „Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop“ (S. 483).

6 Wenn das Home-Verzeichnis des Benutzers für eine andere Linux-Distribution verwendet wurde, entfernten Sie die Datei `Xauthority` aus dem Heimverzeichnis des Benutzers. Melden Sie sich von der Konsole aus mit Strg + Alt + F1 an und führen Sie `rm .Xauthority` als diesen Benutzer aus. Auf diese Weise sollten die X-Authentifizierungsprobleme dieses Benutzers beseitigt werden. Versuchen Sie erneut, sich beim grafischen Desktop anzumelden.

7 Wenn die grafikbasierte Anmeldung nicht möglich ist, melden Sie sich mit Strg + Alt + F1 bei der Konsole an. Versuchen Sie, eine X-Sitzung in einer anderen Anzeige zu starten; die erste (`:0`) wird bereits verwendet:

```
startx -- :1
```

Daraufhin sollten ein grafikbasierter Bildschirm und Ihr Desktop angezeigt werden. Prüfen Sie andernfalls die Protokolldateien des X-Window-Systems (`/var/log/Xorg.`*`anzeigennummer`*`.log`) bzw. die Protokolldateien Ihrer Desktop-Anwendungen (`.xsession-errors` im Home-Verzeichnis des Benutzers) auf Unregelmäßigkeiten hin.

8 Wenn der Desktop aufgrund beschädigter Konfigurationsdateien nicht aufgerufen werden konnte, fahren Sie mit Abschnitt 31.4.4, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“ (S. 482) oder Abschnitt 31.4.5, „Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop“ (S. 483) fort.

31.4.3 Anmeldung bei verschlüsselter Home-Partition fehlgeschlagen

Bei Laptops ist es empfehlenswert, die Home-Partition zu verschlüsseln. Wenn Sie sich bei Ihrem Laptop nicht anmelden können, gibt es dafür normalerweise einen einfachen Grund: Ihre Partition konnte nicht entsperrt werden.

Beim Booten müssen Sie den Passwortsatz eingeben, damit Ihre verschlüsselte Partition entsperrt wird. Wenn Sie den Passwortsatz nicht eingeben, wird der Boot-Vorgang fortgesetzt und die Partition bleibt gesperrt.

Gehen Sie folgendermaßen vor, um die verschlüsselte Partition zu entsperren:

1 Schalten Sie zur Textkonsole um, indem Sie auf Strg + Alt + F1 drücken.

2 Melden Sie sich als `root` an.

3 Starten Sie den Entsperrvorgang erneut mit:

```
/etc/init.d/boot.crypto restart
```

4 Geben Sie Ihren Passwortsatz ein, um die verschlüsselte Partition zu entsperren.

5 Beenden Sie die Textkonsole und wechseln Sie mit Alt + F7 zum Anmeldebildschirm.

6 Melden Sie sich wie gewöhnlich an.

31.4.4 Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop

Wenn dies der Fall ist, sind Ihre GNOME-Konfigurationsdateien vermutlich beschädigt. Mögliche Symptome: Die Tastatur funktioniert nicht, die Geometrie des Bildschirms ist verzerrt oder es ist nur noch ein leeres graues Feld zu sehen. Die wichtige Unterscheidung ist hierbei, dass der Computer normal funktioniert, wenn sich ein anderer Benutzer anmeldet. Das Problem kann in diesem Fall höchstwahrscheinlich verhältnismäßig schnell behoben werden, indem das GNOME-Konfigurationsverzeichnis des Benutzers an einen neuen Speicherort verschoben wird, da GNOME daraufhin ein neues initialisiert. Obwohl der Benutzer GNOME neu konfigurieren muss, gehen keine Daten verloren.

1 Schalten Sie durch Drücken von Strg + Alt + F1 auf eine Textkonsole um.

2 Melden Sie sich mit Ihrem Benutzernamen an.

3 Verschieben Sie die GNOME-Konfigurationsverzeichnisse des Benutzers an einen temporären Speicherort:

```
mv .gconf  .gconf-ORIG-RECOVER
mv .gnome2 .gnome2-ORIG-RECOVER
```

4 Melden Sie sich ab.

5 Melden Sie sich erneut an, führen Sie jedoch keine Anwendungen aus.

6 Stellen Sie Ihre individuellen Anwendungskonfigurationsdaten wieder her (einschließlich der Daten des Evolution-E-Mail-Client), indem Sie das Verzeichnis `~/.gconf-ORIG-RECOVER/apps/` wie folgt in das neue Verzeichnis `~/.gconf` zurückkopieren:

```
cp -a .gconf-ORIG-RECOVER/apps .gconf/
```

Wenn dies die Ursache für die Anmeldeprobleme ist, versuchen Sie, nur die kritischen Anwendungsdaten wiederherzustellen, und konfigurieren Sie die restlichen Anwendungen neu.

31.4.5 Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop

Es gibt mehrere Gründe dafür, warum sich Benutzer nicht bei einem KDE-Desktop anmelden können. Beschädigte Cache-Daten sowie beschädigte KDE-Desktop-Konfigurationsdateien können zu Problemen bei der Anmeldung führen.

Cache-Daten werden beim Desktop-Start zur Leistungssteigerung herangezogen. Wenn diese Daten beschädigt sind, wird der Startvorgang nur sehr langsam oder gar nicht ausgeführt. Durch das Entfernen dieser Daten müssen die Desktop-Startroutinen ganz am Anfang beginnen. Dies nimmt mehr Zeit als ein normaler Startvorgang in Anspruch, die Daten sind jedoch im Anschluss intakt und der Benutzer kann sich anmelden.

Wenn die Cache-Dateien des KDE-Desktop entfernt werden sollen, geben Sie als `root`-Benutzer folgendes Kommando ein:

```
rm -rf /tmp/kde-user /tmp/ksocket-user
```

Ersetzen Sie *`user`* durch Ihren Benutzernamen. Durch das Entfernen dieser beiden Verzeichnisse werden lediglich die beschädigten Cache-Dateien entfernt. Andere Dateien werden durch dieses Verfahren nicht beeinträchtigt.

Beschädigte Desktop-Konfigurationsdateien können stets durch die anfänglichen Konfigurationsdateien ersetzt werden. Wenn die vom Benutzer vorgenommenen Anpassungen wiederhergestellt werden sollen, kopieren Sie sie, nachdem die Konfiguration mithilfe der standardmäßigen Konfigurationswerte wiederhergestellt wurde, sorgfältig von ihrem temporären Speicherort zurück.

Gehen Sie wie folgt vor, um die beschädigte Desktop-Konfiguration durch die anfänglichen Konfigurationswerte zu ersetzen:

1 Schalten Sie durch Drücken von Strg + Alt + F1 auf eine Textkonsole um.

2 Melden Sie sich mit Ihrem Benutzernamen an.

3 Verschieben Sie das KDE-Konfigurationsverzeichnis sowie die `.skel`-Dateien an einen temporären Speicherort:

- Verwenden Sie die folgenden Kommandos für KDE3:

```
mv .kde  .kde-ORIG-RECOVER
mv .skel .skel-ORIG-RECOVER
```

- Verwenden Sie die folgenden Kommandos für KDE4:

```
mv .kde4  .kde4-ORIG-RECOVER
mv .skel .skel-ORIG-RECOVER
```

4 Melden Sie sich ab.

5 Melden Sie sich erneut an.

6 Kopieren Sie nach dem erfolgreichen Aufruf des Desktop die Konfigurationen des Benutzers in das entsprechende Verzeichnis zurück:

```
cp -a KDEDIR/share .kde/share
```

Ersetzen Sie *`KDEDIR`* durch das Verzeichnis aus Schritt 3 (S. 484).

WICHTIG

Wenn die vom Benutzer vorgenommenen Anpassungen zu den Anmeldeproblemen geführt haben und dies auch weiterhin tun, wiederholen Sie die oben beschriebenen Prozeduren, unterlassen Sie jedoch das Kopieren des Verzeichnisses `.kde/share`.

31.5 Probleme mit dem Netzwerk

Zahlreiche Probleme Ihres Systems stehen möglicherweise mit dem Netzwerk in Verbindung, obwohl zunächst ein anderer Eindruck entsteht. So kann beispielsweise ein Netzwerkproblem die Ursache sein, wenn sich Benutzer bei einem System nicht anmelden können. In diesem Abschnitt finden Sie eine einfache Checkliste, anhand derer Sie die Ursache jeglicher Netzwerkprobleme ermitteln können.

Prozedur 31.6 *Erkennen von Netzwerkproblemen*

Gehen Sie zur Überprüfung der Netzwerkverbindung Ihres Computers folgendermaßen vor:

1 Wenn Sie eine Ethernet-Verbindung nutzen, überprüfen Sie zunächst die Hardware. Vergewissern Sie sich, dass das Netzwerkkabel ordnungsgemäß am Computer und Router (oder Hub etc.) angeschlossen ist. Die Kontrolllämpchen neben dem Ethernet-Anschluss sollten beide leuchten.

Wenn keine Verbindung hergestellt werden kann, testen Sie, ob Ihr Netzwerkkabel funktionstüchtig ist, wenn es mit einem anderen Computer verbunden wird. Wenn dies der Fall ist, ist das Problem auf Ihre Netzwerkkarte zurückzuführen. Wenn Ihre Netzwerkeinrichtung Hubs oder Switches enthält, sind diese möglicherweise auch fehlerhaft.

2 Bei einer drahtlosen Verbindung testen Sie, ob die drahtlose Verbindung von anderen Computern hergestellt werden kann. Ist dies nicht der Fall, sollten Sie das Problem an den Administrator des drahtlosen Netzwerks weiterleiten.

3 Nachdem Sie die grundlegende Netzwerkkonnektivität sichergestellt haben, versuchen Sie zu ermitteln, welcher Dienst nicht reagiert. Tragen Sie die Adressinformationen aller Netzwerkserver zusammen, die Bestandteil Ihrer Einrichtung sind. Suchen Sie sie entweder im entsprechenden YaST-Modul oder wenden Sie sich an Ihren Systemadministrator. In der nachfolgenden Liste sind einige der typischen Netzwerkserver aufgeführt, die Bestandteil einer Einrichtung sind; außerdem finden Sie hier die Symptome eines Ausfalls.

DNS (Namendienst)
: Ein Namendienst, der ausgefallen ist oder Fehlfunktionen aufweist, kann die Funktionalität des Netzwerks auf vielfältige Weise beeinträchtigen. Wenn der lokale Computer hinsichtlich der Authentifizierung von Netzwerkservern

abhängig ist und diese Server aufgrund von Problemen bei der Namenauflösung nicht gefunden werden, können sich die Benutzer nicht einmal anmelden. Computer im Netzwerk, die von einem ausgefallenen Namenserver verwaltet werden, sind füreinander nicht „sichtbar“ und können nicht kommunizieren.

NTP (Zeitdienst)
: Ein NTP-Dienst, der ausgefallen ist oder Fehlfunktionen aufweist, kann die Kerberos-Authentifizierung und die X-Server-Funktionalität beeinträchtigen.

NFS (Dateidienst)
: Wenn eine Anwendung Daten benötigt, die in einem NFS-eingehängten Verzeichnis gespeichert sind, kann sie nicht aufgerufen werden bzw. weist Fehlfunktionen auf, wenn dieser Dienst ausgefallen oder falsch konfiguriert ist. Im schlimmsten Fall wird die persönliche Desktop-Konfiguration eines Benutzers nicht angezeigt, wenn sein Home-Verzeichnis mit dem `.gconf`- bzw. `.kde`-Unterverzeichnis nicht gefunden wird, weil der NFS-Server ausgefallen ist.

Samba (Dateidienst)
: Wenn eine Anwendung Daten benötigt, die in einem Verzeichnis auf einem fehlerhaften Samba-Server gespeichert sind, kann sie nicht aufgerufen werden oder weist Fehlfunktionen auf.

NIS (Benutzerverwaltung)
: Wenn Ihr SUSE Linux Enterprise Desktop-System hinsichtlich der Bereitstellung der Benutzerdaten von einem fehlerhaften NIS-Server abhängig ist, können sich Benutzer nicht bei diesem Computer anmelden.

LDAP (Benutzerverwaltung)
: Wenn Ihr SUSE Linux Enterprise Desktop-System hinsichtlich der Bereitstellung der Benutzerdaten von einem fehlerhaften LDAP-Server abhängig ist, können sich Benutzer nicht bei diesem Computer anmelden.

Kerberos (Authentifizierung)
: Die Authentifizierung funktioniert nicht und die Anmeldung bei den Computern schlägt fehl.

CUPS (Netzwerkdruck)
: Die Benutzer können nicht drucken.

4 Überprüfen Sie, ob die Netzwerkserver aktiv sind und ob Ihre Netzwerkeinrichtung das Herstellern einer Verbindung ermöglicht:

WICHTIG

Das unten beschriebene Fehlersuchverfahren gilt nur für ein einfaches Setup aus Netzwerkserver/-Client, das kein internes Routing beinhaltet. Es wird davon ausgegangen, dass sowohl Server als auch Client Mitglieder desselben Subnetzes sind, ohne dass die Notwendigkeit für weiteres Routing besteht.

4a Mit `ping` *`IP-adresse`* `oder` *`hostname`* (ersetzen Sie *`hostname`* durch den Hostnamen des Servers) können Sie überprüfen, ob die einzelnen Server verfügbar sind und ob vom Netzwerk aus auf sie zugegriffen werden kann. Wenn dieses Kommando erfolgreich ist, besagt dies, dass der von Ihnen gesuchte Host aktiv ist und dass der Namendienst für Ihr Netzwerk vorschriftsmäßig konfiguriert ist.

Wenn beim Ping-Versuch die Meldung `destination host unreachable` zurückgegeben wird, also nicht auf den Ziel-Host zugegriffen werden kann, ist entweder Ihr System oder der gewünschte Server nicht vorschriftsmäßig konfiguriert oder ausgefallen. Überprüfen Sie, ob Ihr System erreichbar ist, indem Sie `ping` *`IP-adresse`* `oder` *`ihr_hostname`* von einem anderen Computer aus ausführen. Wenn Sie von einem anderen Computer aus auf Ihren Computer zugreifen können, ist der Server nicht aktiv oder nicht vorschriftsmäßig konfiguriert.

Wenn beim Ping-Versuch die Meldung `unknown host` zurückgegeben wird, der Host also nicht bekannt ist, ist der Namendienst nicht vorschriftsmäßig konfiguriert oder der verwendete Hostname ist falsch. Weitere Prüfungen dieser Arten finden Sie unter Schritt 4b (S. 487). Wenn der Ping-Versuch weiterhin erfolglos ist, ist entweder Ihre Netzwerkkarte nicht vorschriftsmäßig konfiguriert bzw. Ihre Netzwerk-Hardware ist fehlerhaft.

4b Mit `host` *`hostname`* können Sie überprüfen, ob der Hostname des Servers, mit dem Sie eine Verbindung herstellen möchten, vorschriftsmäßig in eine IP-Adresse übersetzt wird (und umgekehrt). Wenn bei diesem Kommando die IP-Adresse dieses Host zurückgegeben wird, ist der Namendienst aktiv. Wenn es bei diesem `host`-Kommando zu einem Problem kommt, überprüfen

Sie alle Netzwerkkonfigurationsdateien, die für die Namen- und Adressauflösung auf Ihrem Host relevant sind:

`/etc/resolv.conf`
: Mithilfe dieser Datei wissen Sie stets, welchen Namenserver und welche Domäne Sie zurzeit verwenden. Diese Datei kann manuell bearbeitet oder unter Verwendung von YaST oder DHCP automatisch angepasst werden. Die automatische Anpassung ist empfehlenswert. Stellen Sie jedoch sicher, dass diese Datei die nachfolgend angegebene Struktur aufweist und dass alle Netzwerkadressen und Domänennamen richtig sind:

```
search fully_qualified_domain_name
nameserver ipaddress_of_nameserver
```

Diese Datei kann die Adresse eines oder mehrerer Namenserver enthalten, mindestens einer davon muss aber richtig sein, um die Namenauflösung für Ihren Host bereitzustellen. Wenn nötig, können Sie diese Datei auf der Registerkarte „Hostname/DNS“ des YaST-Moduls „Netzwerkeinstellungen“ anpassen.

Wenn Ihre Netzwerkverbindung über DHCP erfolgt, aktivieren Sie DHCP, um die Informationen zum Hostnamen und Namendienst zu ändern, indem Sie im YaST-Modul für den DNS- und Hostnamen die Optionen *Hostnamen über DHCP ändern* und *Namenserver und Suchliste über DHCP aktualisieren* auswählen.

`/etc/nsswitch.conf`
: Aus dieser Datei geht hervor, wo Linux nach Namendienstinformationen suchen soll. Sie sollte folgendes Format aufweisen:

```
 ...
hosts: files dns
networks: files dns
...
```

Der Eintrag `dns` ist von großer Bedeutung. Hiermit wird Linux angewiesen, einen externen Namenserver zu verwenden. Normalerweise werden diese Einträge automatisch von YaST verwaltet, es empfiehlt sich jedoch, dies zu überprüfen.

Wenn alle relevanten Einträge auf dem Host richtig sind, lassen Sie Ihren Systemadministrator die DNS-Serverkonfiguration auf die richtigen

Zoneninformationen hin prüfen. Wenn Sie sichergestellt haben, dass die DNS-Konfiguration auf Ihrem Host und dem DNS-Server richtig ist, überprüfen Sie als Nächstes die Konfiguration Ihres Netzwerks und Netzwerkgeräts.

4c Wenn von Ihrem System keine Verbindung mit dem Netzwerk hergestellt werden kann und Sie Probleme mit dem Namendienst mit Sicherheit als Ursache ausschließen können, überprüfen Sie die Konfiguration Ihrer Netzwerkkarte.

Verwenden Sie das Kommando `ifconfig` *`netzwerkgerät`* (Ausführung als `root`), um zu überprüfen, ob dieses Gerät vorschriftsmäßig konfiguriert ist. Stellen Sie sicher, dass sowohl die `inet address` (inet-Adresse) als auch die `Mask` (Maske) ordnungsgemäß konfiguriert sind. Wenn die IP-Adresse einen Fehler enthält oder die Netzwerkmaske unvollständig ist, kann Ihre Netzwerkkonfiguration nicht verwendet werden. Führen Sie diese Überprüfung im Bedarfsfall auch auf dem Server durch.

4d Wenn der Namensdienst und die Netzwerk-Hardware ordnungsgemäß konfiguriert und aktiv/verfügbar sind, bei einigen externen Netzwerkverbindungen jedoch nach wie vor lange Zeitüberschreitungen auftreten bzw. der Verbindungsaufbau überhaupt nicht möglich ist, können Sie mit `traceroute` *`vollständiger_domänenname`* (Ausführung als `root`) die Netzwerkroute dieser Anforderungen überwachen. Mit diesem Kommando werden sämtliche Gateways (Sprünge) aufgelistet, die eine Anforderung von Ihrem Computer auf ihrem Weg zu ihrem Ziel passiert. Mit ihm wird die Antwortzeit der einzelnen Sprünge (Hops) aufgelistet und es wird ersichtlich, ob dieser Sprung überhaupt erreichbar ist. Verwenden Sie eine Kombination von „traceroute“ und „ping“, um die Ursache des Problems ausfindig zu machen, und informieren Sie die Administratoren.

Nachdem Sie die Ursache Ihres Netzwerkproblems ermittelt haben, können Sie es selbst beheben (wenn es auf Ihrem Computer vorliegt) oder die Administratoren Ihres Netzwerks entsprechend informieren, damit sie die Dienste neu konfigurieren bzw. die betroffenen Systeme reparieren können.

31.5.1 Probleme mit NetworkManager

Grenzen Sie Probleme mit der Netzwerkkonnektivität wie unter Prozedur 31.6, „Erkennen von Netzwerkproblemen“ (S. 485) beschrieben ein. Wenn die Ursache bei NetworkManager zu liegen scheint, gehen Sie wie folgt vor, um Protokolle abzurufen, die Hinweise für den Grund der NetworkManager-Probleme enthalten:

1 Öffnen Sie eine Shell und melden Sie sich als `root` an.

2 Starten Sie NetworkManager neu.

```
rcnetwork restart -o nm
```

3 Öffnen Sie eine Website, beispielsweise `http://www.opensuse.org`, als normaler Benutzer, um zu überprüfen, ob Sie eine Verbindung herstellen können.

4 Erfassen Sie sämtliche Informationen zum Status von NetworkManager in `/var/log/NetworkManager`.

Weitere Informationen zu NetworkManager finden Sie unterKapitel 26, *Verwendung von NetworkManager* (S. 399).

31.6 Probleme mit Daten

Probleme mit Daten treten auf, wenn der Computer entweder ordnungsgemäß gebootet werden kann oder nicht, in jedem Fall jedoch offensichtlich ist, dass Daten auf dem System beschädigt wurden und das System wiederhergestellt werden muss. In dieser Situation muss eine Sicherung Ihrer kritischen Daten durchgeführt werden, damit Sie wieder zu dem Zustand zurückkehren können, in dem sich Ihr System befand, als das Problem auftrat. SUSE Linux Enterprise Desktop bietet spezielle YaST-Module für Systemsicherung und -wiederherstellung sowie ein Rettungssystem, das die externe Wiederherstellung eines beschädigten Systems ermöglicht.

31.6.1 Verwalten von Partitions-Images

In manchen Fällen müssen Sie eine Sicherung einer ganzen Partition oder sogar der gesamten Festplatte erstellen. Im Lieferumfang von Linux ist das Werkzeug `dd` enthal-

ten, das eine exakte Kopie Ihrer Festplatte erstellen kann. In Kombination mit `gzip` wird dabei Speicherplatz gespart.

Prozedur 31.7 *Festplatten sichern und wiederherstellen*

1 Starten Sie eine Shell als `root`-Benutzer.

2 Wählen Sie das Quellgerät aus. Typischerweise lautet es wie `/dev/sda` (bezeichnet als *SOURCE*).

3 Entscheiden Sie, wo das Image gespeichert werden soll (bezeichnet als *BACKUP_PATH*). Der Speicherort darf sich nicht auf dem Quellgerät befinden. Mit anderen Worten: Wenn Sie eine Sicherung von `/dev/sda` erstellen, muss das Image nicht unter `/dev/sda` gespeichert werden.

4 Führen Sie die Kommandos zur Erstellung einer komprimierten Image-Datei aus:

```
dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
```

5 Stellen Sie die Festplatte mithilfe der folgenden Kommandos wieder her:

```
gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
```

Wenn Sie nur eine Partition sichern müssen, ersetzen Sie den Platzhalter *SOURCE* durch die entsprechende Partition. In diesem Fall kann sich Ihre Image-Datei auf derselben Festplatte befinden, allerdings in einer anderen Partition.

31.6.2 Sichern kritischer Daten

Systemsicherungen können mithilfe des Yast-Moduls für Systemsicherungen problemlos vorgenommen werden.

1 Rufen Sie YaST als `root` -Benutzer auf und wählen Sie *System* > *Sicherungskopie der Systembereiche*.

2 Erstellen Sie ein Sicherungsprofil mit allen für die Sicherung erforderlichen Details, dem Dateinamen der Archivdatei, dem Umfang sowie dem Sicherungstyp:

2a Wählen Sie *Profilverwaltung* > *Hinzufügen*.

2b Geben Sie einen Namen für das Archiv ein.

2c Geben Sie den Pfad für den Speicherort der Sicherung ein, wenn Sie lokal über eine Sicherung verfügen möchten. Damit Ihre Sicherung auf einem Netzwerkserver archiviert werden kann (über NFS), geben Sie die IP-Adresse oder den Namen des Servers und des Verzeichnisses für die Speicherung Ihres Archivs an.

2d Bestimmen Sie den Archivtyp und klicken Sie dann auf *Weiter*.

2e Bestimmen Sie die zu verwendenden Sicherungsoptionen; geben Sie beispielsweise an, ob Dateien gesichert werden sollen, die keinem Paket zugehörig sind, und ob vor der Erstellung des Archivs eine Liste der Dateien angezeigt werden soll. Legen Sie außerdem fest, ob geänderte Dateien durch den zeitintensiven MDS-Mechanismus identifiziert werden sollen.

Mit *Erweitert* gelangen Sie in ein Dialogfeld für die Sicherung ganzer Festplattenbereiche. Diese Option hat zurzeit nur für das Ext2-Dateisystem Gültigkeit.

2f Legen Sie abschließend die Suchoptionen fest, um bestimmte Systembereiche von der Sicherung auszuschließen, die nicht gesichert werden müssen, beispielsweise Lock- oder Cache-Dateien. Fügen Sie Einträge hinzu, bearbeiten oder löschen Sie sie, bis die Liste Ihren Vorstellungen entspricht, und schließen Sie das Dialogfeld mit *OK*.

3 Nachdem Sie die Profileinstellungen festgelegt haben, können Sie die Sicherung umgehend mit *Sicherungskopie erstellen* beginnen oder die automatische Sicherung konfigurieren. Sie können auch weitere Profile erstellen, die auf andere Zwecke zugeschnitten sind.

Zum Konfigurieren der automatischen Sicherung für ein bestimmtes Profil gehen Sie wie folgt vor:

1 Wählen Sie im Menü *Profilverwaltung* die Option *Automatische Sicherungskopie* aus.

2 Wählen Sie *Sicherungskopie automatisch starten* aus.

3. Legen Sie die Sicherungshäufigkeit fest. Wählen Sie *Täglich*, *Wöchentlich* oder *Monatlich* aus.

4. Legen Sie die Startzeit für die Sicherung fest. Diese Einstellungen werden durch die ausgewählte Sicherungshäufigkeit bestimmt.

5. Geben Sie an, ob alte Sicherungen beibehalten werden sollen, und wenn ja, wie viele. Wenn eine automatisch generierte Statusmeldung bezüglich des Sicherungsvorgangs ausgegeben werden soll, aktivieren Sie *Mail mit Zusammenfassung an Benutzer 'root' senden*.

6. Klicken Sie auf *OK*, um die Einstellungen zu speichern. Danach wird die erste Sicherung zum angegebenen Zeitpunkt gestartet.

31.6.3 Wiederherstellen einer Systemsicherung

Mithilfe des YaST-Moduls für die Systemwiederherstellung kann die Systemkonfiguration anhand einer Sicherung wiederhergestellt werden. Sie können entweder die gesamte Sicherung wiederherstellen oder bestimmte Komponenten auswählen, die beschädigt wurden und wieder in ihren alten Zustand zurückversetzt werden sollen.

1. Wählen Sie die Optionsfolge *YaST > System > System wiederherstellen*.

2. Geben Sie den Speicherort der Sicherungsdatei ein. Hierbei kann es sich um eine lokale Datei, um eine im Netzwerk eingehängte Datei oder um eine Datei auf einem Wechselmedium handeln, beispielsweise einer Diskette oder DVD. Klicken Sie anschließend auf *Weiter*.

   Im nachfolgenden Dialogfeld ist eine Zusammenfasung der Archiveigenschaften zu sehen, beispielsweise Dateinamen, Erstellungsdatum, Sicherungstyp sowie optionale Kommentare.

3. Überprüfen Sie den archivierten Inhalt, indem Sie auf *Inhalt des Archivs klicken*. Mit *OK* kehren Sie zum Dialogfeld *Eigenschaften des Archivs* zurück.

4. *Mit* Optionen für Experten gelangen Sie in ein Dialogfeld, in dem Sie den Wiederherstellungsvorgang präzisieren können. Kehren Sie zum Dialogfeld *Eigenschaften des Archivs* zurück, indem Sie auf *OK* klicken.

5 Klicken Sie auf *Weiter*, um die wiederherzustellenden Pakete anzuzeigen. Mit *Übernehmen* werden alle Dateien im Archiv wiederhergestellt. Mit den Schaltflächen *Alle auswählen*, *Alle abwählen* und *Dateien wählen* können Sie Ihre Auswahl präzisieren. Verwenden Sie die Option *RPM-Datenbank wiederherstellen* nur, wenn die RPM-Datenbank beschädigt oder gelöscht wurde und in der Sicherung enthalten ist.

6 Wenn Sie auf *Übernehmen* klicken, wird die Sicherung wiederhergestellt. Wenn der Wiederherstellungsvorgang abgeschlossen ist, schließen Sie das Modul mit *Verlassen*.

31.6.4 Wiederherstellen eines beschädigten Systems

Ein System kann aus mehreren Gründen nicht aktiviert und ordnungsgemäß betrieben werden. Zu den häufigsten Gründen zählen ein beschädigtes Dateisystem nach einem Systemabsturz, beschädigte Konfigurationsdateien oder eine beschädigte Bootloader-Konfiguration.

SUSE Linux Enterprise Desktop bietet zwei verschiedene Methoden zur Behebung dieser Situationen. Sie können entweder die YaST-Systemreparatur verwenden oder das Rettungssystem booten. Die folgenden Abschnitte befassen sich mit beiden Methoden zur Systemreparatur.

31.6.4.1 Verwenden der YaST-Systemreparatur

ANMERKUNG: Tastatur- und Spracheinstellungen

Wenn Sie die Spracheinstellungen nach dem Booten ändern, wird Ihre Tastatur ebenfalls angepasst.

Vor dem Start des YaST-Moduls zur Systemreparatur sollten Sie ermitteln, in welchem Modus das Modul ausgeführt werden sollte, damit es am besten Ihren Bedürfnissen entspricht. Je nach dem Schweregrad und der Ursache des Systemausfalls (sowie Ihren Fachkenntnissen) können Sie zwischen drei verschiedenen Modi wählen.

Automatische Reparatur

Wenn Ihr System aufgrund einer unbekannten Ursache ausgefallen ist und Sie nicht wissen, welcher Teil des Systems für den Ausfall verantwortlich ist, sollten Sie die *Automatische Reparatur* verwenden. Eine umfassende automatische Prüfung wird

an allen Komponenten des installierten Systems durchgeführt. Eine detaillierte Beschreibung dieses Verfahrens finden Sie in „Automatische Reparatur“ (S. 495).

Benutzerdefinierte Reparatur
: Wenn Ihr System ausgefallen ist und Sie bereits wissen, an welcher Komponente es liegt, können Sie die langwierige Systemprüfung von *Automatische Reparatur* abkürzen, indem Sie den Bereich der Systemanalyse auf die betreffenden Komponenten beschränken. Wenn die Systemmeldungen vor dem Ausfall beispielsweise auf einen Fehler mit der Paketdatenbank hindeuten, können Sie das Analyse- und Reparaturverfahren so einschränken, dass nur dieser Aspekt des Systems überprüft und wiederhergestellt wird. Eine detaillierte Beschreibung dieses Verfahrens finden Sie in „Benutzerdefinierte Reparatur“ (S. 497).

Expertenwerkzeuge
: Wenn Sie bereits eine klare Vorstellung davon haben, welche Komponente ausgefallen ist und wie dieser Fehler behoben werden kann, können Sie die Analyseläufe überspringen und die für die Reparatur der betreffenden Komponente erforderlichen Werkzeuge unmittelbar anwenden. Detaillierte Informationen finden Sie in „Expertenwerkzeuge“ (S. 498).

Wählen Sie einen der oben beschriebenen Reparaturmodi aus und setzen Sie die Systemreparatur, wie in den folgenden Abschnitten beschrieben, fort.

Automatische Reparatur

Um den Modus für automatische Reparatur der YaST-Systemreparatur zu starten, gehen Sie wie folgt vor:

1 Legen Sie das Installationsmedium von SUSE Linux Enterprise Desktop in das DVD-Laufwerk ein.

2 Booten Sie das System neu.

3 Wählen Sie im Boot-Fenster die Option *Installiertes System reparieren* aus.

4 Bestätigen Sie die Lizenzvereinbarung, und klicken Sie auf *Weiter*.

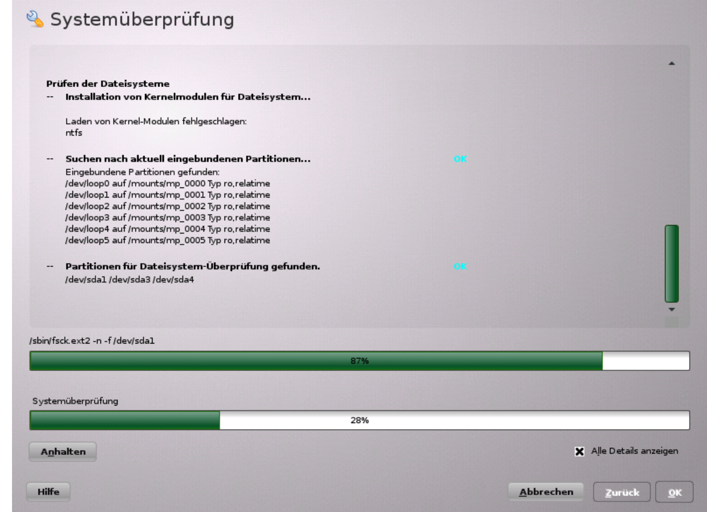
5 Wählen Sie *Automatische Reparatur*.

YaST startet nun eine umfassende Analyse des installierten Systems. Der Verlauf des Vorgangs wird unten auf dem Bildschirm mit zwei Verlaufsbalken angezeigt.

Der obere Balken zeigt den Verlauf des aktuell ausgeführten Tests. Der untere Balken zeigt den Gesamtverlauf des Analysevorgangs. Im Protokollfenster im oberen Abschnitt werden der aktuell ausgeführte Test und sein Ergebnis aufgezeichnet. Weitere Informationen hierzu finden Sie unter Abbildung 31.4, „Modus „Automatische Reparatur““ (S. 496).

Abbildung 31.4 *Modus „Automatische Reparatur“*





Die folgenden Haupttestläufe werden bei jeder Ausführung durchgeführt. Sie enthalten jeweils eine Reihe einzelner Untertests:

Partitionstabellen prüfen
: Überprüft Validität und Kohärenz der Partitionstabellen aller erkannten Festplatten.

Prüfen des Swap-Bereichs
: Die Swap-Partitionen des installierten Systems werden erkannt, getestet und gegebenenfalls zur Aktivierung angeboten. Dieses Angebot sollte angenommen werden, um eine höhere Geschwindigkeit für die Systemreparatur zu erreichen.

Prüfen der Dateisysteme
: Alle gefundenen Dateisysteme werden einer dateisystem-spezifischen Prüfung unterworfen.

Prüfen der fstab-Einträge
: Die Einträge in der Datei werden auf Vollständigkeit und Konsistenz überprüft. Alle gültigen Partitionen werden eingehängt.

Paketdatenbank prüfen
: Mit dieser Option wird überprüft, ob alle für den Betrieb einer Minimalinstallation erforderlichen Pakete vorliegen. Es ist zwar möglich, die Basispakete ebenfalls zu analysieren, dies dauert jedoch aufgrund ihrer großen Anzahl sehr lange.

Prüfen der Bootloader-Konfiguration
: Die Bootloader-Konfiguration des installierten Systems (GRUB oder LILO) wird auf Vollständigkeit und Kohärenz überprüft. Boot- und Root-Geräte werden untersucht, und die Verfügbarkeit der initrd-Module wird überprüft.

6 Immer wenn ein Fehler gefunden wird, wird der Vorgang angehalten und es öffnet sich ein Dialogfeld, in dem die Details und die möglichen Lösungen beschrieben werden.

Lesen Sie die Bildschirmmeldungen genau durch, bevor Sie die vorgeschlagene Reparaturmöglichkeit akzeptieren. Wenn Sie eine vorgeschlagene Lösung ablehnen, werden keine Änderungen am System vorgenommen.

7 Klicken Sie nach erfolgreicher Beendigung des Reparaturvorgangs auf *OK* und *Verlassen* und entfernen Sie die Installationsmedien. Das System wird automatisch neu gebootet.

Benutzerdefinierte Reparatur

Um den Modus *Benutzerdefinierte Reparatur* zu starten und ausgewählte Komponenten des installierten Systems zu prüfen, gehen Sie wie folgt vor:

1 Legen Sie das Installationsmedium von SUSE Linux Enterprise Desktop in das DVD-Laufwerk ein.

2 Booten Sie das System neu.

3 Wählen Sie im Boot-Fenster die Option *Installiertes System reparieren* aus.

4 Bestätigen Sie die Lizenzvereinbarung, und klicken Sie auf *Weiter*.

5 Wählen Sie *Benutzerdefinierte Reparatur*.

   Bei Auswahl von *Benutzerdefinierte Reparatur* wird eine Liste der Testläufe angezeigt, die zunächst alle für die Ausführung markiert sind. Der Gesamttestbereich entspricht dem der automatischen Reparatur. Wenn Sie bereits Systembereiche kennen, in denen kein Schaden vorliegt, heben Sie die Markierung der entsprechenden Tests auf. Beim Klicken auf *Weiter* wird ein engeres Testverfahren gestartet, für dessen Ausführung vermutlich wesentlich weniger Zeit erforderlich ist.

   Nicht alle Testgruppen können individuell angewendet werden. Die Analyse der fstab-Einträge ist stets an eine Untersuchung der Dateisysteme gebunden, einschließlich bestehender Swap-Partitionen. YaST löst solche Abhängigkeiten automatisch auf, indem es die kleinste Zahl an erforderlichen Testläufen auswählt. YaST unterstützt keine verschlüsselten Partitionen. Falls eine verschlüsselte Partition vorhanden ist, informiert YaST Sie darüber.

6 Immer wenn ein Fehler gefunden wird, wird der Vorgang angehalten und es öffnet sich ein Dialogfeld, in dem die Details und die möglichen Lösungen beschrieben werden.

   Lesen Sie die Bildschirmmeldungen genau durch, bevor Sie die vorgeschlagene Reparaturmöglichkeit akzeptieren. Wenn Sie eine vorgeschlagene Lösung ablehnen, werden keine Änderungen am System vorgenommen.

7 Klicken Sie nach erfolgreicher Beendigung des Reparaturvorgangs auf *OK* und *Verlassen* und entfernen Sie die Installationsmedien. Das System wird automatisch neu gebootet.

Expertenwerkzeuge

Wenn Sie mit SUSE Linux Enterprise Desktop vertraut sind und bereits eine genaue Vorstellung davon haben, welche Komponenten in Ihrem System repariert werden müssen, können Sie die Systemanalyse überspringen und die Werkzeuge direkt anwenden.

Um die Funktion *Expertenwerkzeuge* der YaST-Systemreparatur zu verwenden, fahren Sie wie folgt fort:

1 Legen Sie das Installationsmedium von SUSE Linux Enterprise Desktop in das DVD-Laufwerk ein.

2 Booten Sie das System neu.

3 Wählen Sie im Boot-Fenster die Option *Installiertes System reparieren* aus.

4 Bestätigen Sie die Lizenzvereinbarung, und klicken Sie auf *Weiter*.

5 Klicken Sie auf *Expertenwerkzeuge* und wählen Sie dann eine Reparaturoption aus.

6 Klicken Sie nach erfolgreicher Beendigung des Reparaturvorgangs auf *OK* und *Verlassen* und entfernen Sie die Installationsmedien. Das System wird automatisch neu gebootet.

Unter *Expertenwerkzeugen* stehen folgende Optionen zum Reparieren des fehlerhaften Systems zur Verfügung:

Neuen Bootloader installieren
Dadurch wird das Konfigurationsmodul für den YaST-Bootloader gestartet. Einzelheiten finden Sie in Abschnitt 12.2, „Konfigurieren des Bootloaders mit YaST" (S. 164).

Installiertes System booten
Versuchen Sie, ein bereits installiertes Linux-System zu booten.

Partitionierer starten
Mit dieser Option wird das Expertenwerkzeug für die Partitionierung in YaST gestartet.

Reparatur des Dateisystems
Mit dieser Option werden die Dateisysteme Ihrer installierten Systeme überprüft. Ihnen wird zunächst eine Auswahl aller erkannten Partitionen angeboten, aus denen Sie die zu überprüfenden auswählen können.

Verlorene Partitionen wiederherstellen
Sie können versuchen, beschädigte Partitionstabellen zu rekonstruieren. Zunächst wird eine Liste der erkannten Festplatten zur Auswahl angeboten. Durch Klicken auf *OK* wird die Untersuchung gestartet. Dies kann je nach der Geschwindigkeit Ihres Computers und der Größe und Geschwindigkeit der Festplatte einige Zeit in Anspruch nehmen.

WICHTIG: ***Rekonstruktion von Partitionstabellen***

Die Rekonstruktion einer Partitionstabellen ist ein komplizierter Vorgang. YaST versucht, verloren gegangene Partitionen durch Analyse der Datensektoren der Festplatte wiederherzustellen. Die verlorenen Partitionen werden, wenn sie erkannt werden, zur neu erstellten Partitionstabelle hinzugefügt. Dies ist jedoch nicht in allen vorstellbaren Fällen erfolgreich.

Systemeinstellungen auf Diskette speichern
: Mit dieser Option werden wichtige Systemdateien auf eine Diskette gespeichert. Wenn eine dieser Dateien beschädigt wird, kann Sie von der Diskette wiederhergestellt werden.

Installierte Software prüfen
: Mit dieser Option werden die Konsistenz der Paketdatenbank und die Verfügbarkeit der wichtigsten Pakete überprüft. Mit diesem Werkzeug können alle beschädigten Installationspakete wiederhergestellt werden.

31.6.4.2 Verwenden des Rettungssystems

SUSE Linux Enterprise Desktop umfasst ein Rettungssystem. Das Rettungssystem ist ein kleines Linux-System, das auf einen RAM-Datenträger geladen und als Root-Dateisystem eingehängt werden kann. Es ermöglicht Ihnen so den externen Zugriff auf Ihre Linux-Partitionen. Mithilfe des Rettungssystems kann jeder wichtige Aspekt Ihres Systems wiederhergestellt oder geändert werden:

- Jede Art von Konfigurationsdatei kann bearbeitet werden.
- Das Dateisystem kann auf Fehler hin überprüft und automatische Reparaturvorgänge können gestartet werden.
- Der Zugriff auf das installierte System kann in einer „change-root“-Umgebung erfolgen.
- Die Bootloader-Konfiguration kann überprüft, geändert und neu installiert werden.
- Eine Wiederherstellung ab einem fehlerhaft installierten Gerätetreiber oder einem nicht verwendbaren Kernel kann durchgeführt werden.

- Die Größe von Partitionen kann mithilfe des parted-Kommandos verändert werden. Weitere Informationen zu diesem Werkzeug finden Sie auf der Website von GNU Parted `http://www.gnu.org/software/parted/parted.html`.

Das Rettungssystem kann aus verschiedenen Quellen und von verschiedenen Speicherorten geladen werden. Am einfachsten lässt sich das Rettungssystem vom Original-Installationsmedium booten:

1 Legen Sie das Installationsmedium in Ihr DVD-Laufwerk ein.

2 Booten Sie das System neu.

3 Drücken Sie im Boot-Fenster F4 und wählen Sie *DVD-ROM*. Wählen Sie dann im Hauptmenü die Option *Rettungssystem*.

4 Geben Sie an der Eingabeaufforderung `Rescue:root` ein. Ein Passwort ist nicht erforderlich.

Wenn Ihnen kein DVD-Laufwerk zur Verfügung steht, können Sie das Rettungssystem von einer Netzwerkquelle booten. Das nachfolgende Beispiel bezieht sich auf das entfernte Booten – wenn Sie ein anderes Boot-Medium verwenden, beispielsweise eine DVD, ändern Sie die Datei `info` entsprechend, und führen Sie den Boot-Vorgang wie bei einer normalen Installation aus.

1 Geben Sie die Konfiguration Ihres PXE-Boot-Setups ein und fügen Sie die Zeilen `install=`*`protocol`*`://`*`instsource`* und `rescue=1` hinzu. Wenn das Reparatursystem gestartet werden soll, verwenden Sie stattdessen `repair=1`. Wie bei einer normalen Installation steht *`protokoll`* für eines der unterstützten Netzwerkprotokolle (NFS, HTTP, FTP usw.) und *`instquelle`* für den Pfad zur Netzwerkinstallationsquelle.

2 Booten Sie das System mit „Wake on LAN“, wie im Abschnitt „Wake-on-LAN“ (Kapitel 11, *Installation mit entferntem Zugriff*, ↑*Bereitstellungshandbuch*) erläutert.

3 Geben Sie an der Eingabeaufforderung `Rescue:root` ein. Ein Passwort ist nicht erforderlich.

Sobald Sie sich im Rettungssystem befinden, können Sie die virtuellen Konsolen verwenden, die über die Tasten Alt + F1 bis Alt + F6 aufgerufen werden.

Eine Shell und viele andere hilfreiche Dienstprogramme, beispielsweise das mount-Programm, stehen im Verzeichnis `/bin` zur Verfügung. Das Verzeichnis `sbin` enthält wichtige Datei- und Netzwerkdienstprogramme, mit denen das Dateisystem überprüft und repariert werden kann. In diesem Verzeichnis finden Sie auch die wichtigsten Binärdateien für die Systemwartung, beispielsweise fdisk, mkfs, mkswap, mount, mount, init und shutdown sowie ifconfig, ip, route und netstat für die Netzwerkwartung. Das Verzeichnis `/usr/bin` enthält den vi-Editor, find, less sowie ssh.

Die Systemmeldungen können über das Kommando `dmesg` angezeigt werden; Sie können auch die Datei `/var/log/messages` zurate ziehen.

Überprüfen und Bearbeiten von Konfigurationsdateien

Als Beispiel für eine Konfiguration, die mithilfe des Rettungssystems repariert werden kann, soll eine beschädigte Konfigurationsdatei dienen, die das ordnungsgemäße Booten des Systems verhindert. Dieses Problem kann mit dem Rettungssystem behoben werden.

Gehen Sie zum Bearbeiten einer Konfigurationsdatei folgendermaßen vor:

1. Starten Sie das Rettungssystem mithilfe einer der oben erläuterten Methoden.

2. Verwenden Sie zum Einhängen eines Root-Dateisystems unter `/dev/sda6` in das Rettungssystem folgendes Kommando:

   ```
   mount /dev/sda6 /mnt
   ```

   Sämtliche Verzeichnisse des Systems befinden sich nun unter `/mnt`

3. Wechseln Sie in das eingehängte Root -Dateisystem:

   ```
   cd /mnt
   ```

4. Öffnen Sie die fehlerhafte Konfigurationsdatei im vi-Editor. Passen Sie die Konfiguration an und speichern Sie sie.

5. Hängen Sie das Root-Dateisystem aus dem Rettungssystem aus:

   ```
   umount /mnt
   ```

6. Booten Sie den Computer neu.

Reparieren und Überprüfen von Dateisystemen

Generell ist das Reparieren von Dateisystemen auf einem zurzeit aktiven System nicht möglich. Bei ernsthaften Problemen ist möglicherweise nicht einmal das Einhängen Ihres Root-Dateisystems möglich und das Booten des Systems endet unter Umständen mit einer so genannten „Kernel-Panic“. In diesem Fall ist nur die externe Reparatur des Systems möglich. Für diese Aufgabe wird die Verwendung der YaST-Systemreparatur dringend empfohlen (siehe Abschnitt 31.6.4.1, „Verwenden der YaST-Systemreparatur“ (S. 494)). Wenn Sie jedoch die manuelle Überprüfung bzw. Reparatur des Dateisystems durchführen müssen, booten Sie das Rettungssystem. Es enthält die Dienstprogramme für die Überprüfung und Reparatur der Dateisysteme `btrfs`, `ext2`, `ext3`, `ext4`, `reiserfs`, `xfs`, `dosfs` und `vfat`.

Zugriff auf das installierte System

Wenn Sie vom Rettungssystem aus auf das installierte System zugreifen müssen, ist dazu eine *change-root*-Umgebung erforderlich. Beispiele: Bearbeiten der Bootloader-Konfiguration oder Ausführen eines Dienstprogramms zur Hardwarekonfiguration.

Gehen Sie zur Einrichtung einer change-root-Umgebung, die auf dem installierten System basiert, folgendermaßen vor:

1 Hängen Sie zunächst die Root-Partition des installierten Systems und des Gerätedateisystems ein (ändern Sie den Gerätenamen entsprechend Ihren aktuellen Einstellungen):

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

2 Nun können Sie per „change-root“ in die neue Umgebung wechseln:

```
chroot /mnt
```

3 Hängen Sie dann `/proc` und `/sys` ein:

```
mount /proc
mount /sys
```

4 Abschließend hängen Sie die restlichen Partitionen vom installierten System ein:

```
mount -a
```

5 Nun können Sie auf das installierte System zugreifen. Hängen Sie vor dem Reboot des Systems die Partitionen mit `umount -a` aus und verlassen Sie die „change-root“-Umgebung mit `exit`.

WARNUNG: Einschränkungen

Obwohl Sie über uneingeschränkten Zugriff auf die Dateien und Anwendungen des installierten Systems verfügen, gibt es einige Beschränkungen. Der Kernel, der ausgeführt wird, ist der Kernel, der mit dem Rettungssystem gebootet wurde, nicht mit der change-root-Umgebung. Er unterstützt nur essenzielle Hardware, und das Hinzufügen von Kernel-Modulen über das installierte System ist nur möglich, wenn die Kernel-Versionen genau übereinstimmen. Überprüfen Sie immer die Version des aktuell ausgeführten (Rettungssytem-) Kernels mit `uname -r` und stellen Sie fest, ob im Verzeichnis `/lib/modules` in der change-root-Umgebung passende Unterverzeichnisse vorhanden sind. Wenn dies der Fall ist, können Sie die installierten Module verwenden. Andernfalls müssen Sie diese in den richtigen Version von einem anderen Medium, z. B. einem USB-Stick, bereitstellen. In den meisten Fällen weicht die Kernel-Version des Rettungssystems von der des installierten ab – dann können Sie z. B. nicht einfach auf eine Soundkarte zugreifen. Der Aufruf einer grafischen Bedienoberfläche ist ebenfalls nicht möglich.

Beachten Sie außerdem, dass Sie die „change-root“-Umgebung verlassen, wenn Sie die Konsole mit Alt + F1 bis Alt + F6 umschalten.

Bearbeiten und erneutes Installieren des Bootloader

In einigen Fällen kann ein System aufgrund einer beschädigten Bootloader-Konfiguration nicht gebootet werden. Die Start-Routinen sind beispielsweise nicht in der Lage, physische Geräte in die tatsächlichen Speicherorte im Linux-Dateisystem zu übersetzen, wenn der Bootloader nicht ordnungsgemäß funktioniert.

Gehen Sie wie folgt vor, um die Bootloader-Konfiguration zu überprüfen und den Bootloader neu zu installieren:

1 Führen Sie die unter „Zugriff auf das installierte System“ (S. 503) erläuterten erforderlichen Schritte für den Zugriff auf das installierte System aus.

2. Vergewissern Sie sich, dass die nachfolgend angegebenen Dateien gemäß den in Kapitel 12, *Der Bootloader GRUB* (S. 151) erläuterten GRUB-Konfigurationsgrundlagen ordnungsgemäß konfiguriert sind, und wenden Sie Fixes an, falls erforderlich.

   - `/etc/grub.conf`
   - `/boot/grub/device.map`
   - `/boot/grub/menu.lst`
   - `/etc/sysconfig/bootloader`

3. Installieren Sie den Bootloader mit folgender Kommandosequenz neu:

   ```
   grub --batch < /etc/grub.conf
   ```

4. Hängen Sie die Partitionen aus, melden Sie sich von der „change-root"-Umgebung ab und führen Sie den Reboot des Systems durch:

   ```
   umount -a
   exit
   reboot
   ```

Korrektur der Kernel-Installation

Ein Kernel-Update kann einen neuen Fehler verursachen, der sich auf Ihr System auswirken kann. Es kann z. B. ein Treiber für eine Hardwarekomponente in Ihrem System falsch sein, weshalb Sie nicht auf die Komponente zugreifen und diese nicht verwenden können. Kehren Sie in diesem Fall zum letzten funktionierenden Kernel zurück (sofern er im System verfügbar ist) oder installieren Sie den Original-Kernel vom Installationsmedium.

TIPP: So erhalten Sie die aktuellsten Kernels nach dem Update

Um Fehler beim Booten durch eine fehlerhaften Kernel-Aktualisierung zu vermeiden, können Sie die Multiversionsfunktion für Kernel nutzen und `libzypp` mitteilen, welche Kernel Sie nach der Aktualisierung erhalten möchten.

Damit z. B. immer die beiden letzten Kernels und der aktuell ausgeführte erhalten bleiben, fügen Sie

```
multiversion.kernels = latest,latest-1,running
```

zur Datei `/etc/zypp/zypp.conf` hinzu.

Ähnlich verhält es sich, wenn Sie einen defekten Treiber für ein nicht durch SUSE Linux Enterprise Desktop unterstütztes Gerät neu installieren oder aktualisieren müssen. Wenn z. B. ein Hardwarehersteller ein bestimmtes Gerät verwendet, wie einen Hardware-RAID-Controller, für den es erforderlich ist, dass ein Binärtreiber durch das Betriebssystem erkannt wird. Der Hersteller veröffentlicht in der Regel ein Treiberupdate mit der korrigierten oder aktualisierten Version des benötigten Treibers.

In beiden Fällen müssen Sie im Rettungsmodus auf das installierte System zugreifen und das mit dem Kernel zusammenhängende Problem beheben, da das System andernfalls nicht korrekt booten wird:

1. Booten Sie von den SUSE Linux Enterprise Desktop-Installationsmedien.

2. Überspringen Sie diese Schritt, wenn Sie eine Wiederherstellung nach einer fehlerhaften Kernel-Aktualisierung durchführen. Wenn Sie eine Driver Update Disk (DUD) verwenden, drücken Sie F6, um die Treiberaktualisierung nach der Anzeige des Bootmenüs zu laden, wählen Sie den Pfad oder die URL für die Treiberaktualisierung aus und bestätigen Sie die Auswahl mit *Ja*.

3. Wählen Sie im Bootmenü *Rettungssystem* aus und drücken Sie die Eingabetaste. Wenn Sie eine DUD verwenden, werden Sie aufgefordert, den Speicherplatz der Treiberaktualisierung anzugeben.

4. Geben Sie an der Eingabeaufforderung `Rescue:root` ein. Ein Passwort ist nicht erforderlich.

5. Hängen Sie das Zielsystem manuell ein und führen Sie „change root“ in die neue Umgebung durch. Weitere Informationen finden Sie unter „Zugriff auf das installierte System“ (S. 503).

6. Wenn Sie eine DUD verwenden, installieren oder aktualisieren Sie das fehlerhafte Treiberpaket. Stellen Sie stets sicher, dass die installierte Kernel-Version exakt mit der Version des Treibers übereinstimmt, den Sie installieren möchten.

   Wenn Sie eine fehlerhafte Installation einer Treiberaktualisierung korrigieren, können Sie nach dem folgenden Verfahren den Originaltreiber vom Installationsmedium installieren.

6a Identifizieren Sie Ihr DVD-Laufwerk mit `hwinfo --cdrom` und hängen Sie es mit `mount /dev/sr0 /mnt` ein.

6b Navigieren Sie zum Verzeichnis, in dem Ihre Kernel-Dateien auf der DVD gespeichert sind, z. B. `cd /mnt/suse/x86_64/`.

6c Installieren Sie die benötigten `kernel-*`-, `kernel-*-base`- und `kernel-*-extra`-Pakete mit dem Kommando `rpm -i`.

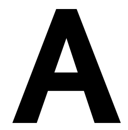
6d Prüfen Sie nach Abschluss der Installation, ob für den neu installierten Kernel ein neuer Menüeintrag zur Bootloader-Konfigurationsdatei (`/boot/grub/menu.lst` für `grub`) hinzugefügt wurde.

7 Aktualisieren Sie Konfigurationsdateien und initialisieren Sie den Bootloader gegebenenfalls neu. Weitere Informationen finden Sie in „Bearbeiten und erneutes Installieren des Bootloader“ (S. 504).

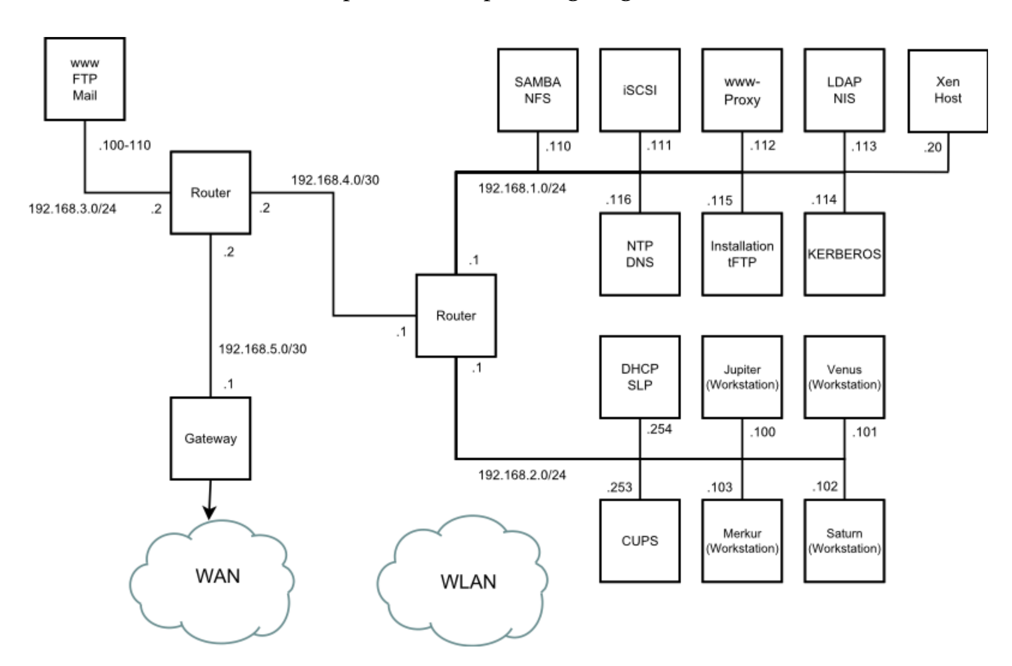
8 Entfernen Sie alle bootbaren Medien aus dem Systemlaufwerk und booten Sie neu.



Ein Beispielnetzwerk



Dieses Beispielnetzwerk wird in allen Kapiteln über das Netzwerk in der Dokumentation zu SUSE® Linux Enterprise Desktop herangezogen.





GNU Licenses

B

This appendix contains the GNU Free Documentation License version 1.2.

GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

